Wireless LAN USB Adapter

User Manual 1.0

© 2010

Contents

1. Windows Wireless Utility 3
   - 1.1 Windows Zero Configuration for XP 3
     - 1.1.1 Ralink Wireless Utility and Windows Zero Configuration 3
     - 1.1.2 Windows Zero Configuration (WZC) 4
   - 1.2 Windows AutoConfig Service for Vista 9
     - 1.2.1 Ralink Wireless Utility and Windows AutoConfig Service 9
     - 1.2.2 Windows AutoConfig Service 10
2. Ralink Wireless Utility (RaUI) 17
   - 2.1 Start 17
     - 2.1.1 Start RaUI 17
   - 2.2 Profile 20
     - 2.2.1 Profile 20
     - 2.2.2 Add/Edit Profile 21
     - 2.2.3 Example to Add Profile in Profile 24
     - 2.2.4 Pre-logon Connect 26
   - 2.3 Network 26
     - 2.3.1 Network 26
     - 2.3.2 Example on Adding Profile in Network 29
   - 2.4 Advanced 30
     - 2.4.1 Advanced 30
     - 2.4.2 Certificate Management 31
   - 2.5 Link Information 32
     - 2.5.1 Link Status 32
     - 2.5.2 Throughput 33
     - 2.5.3 Statistics 33
   - 2.6 About 34
     - 2.6.1 About 34
   - 2.7 WPS 35
     - 2.7.1 WPS 35
     - 2.7.2 Example to Add to Registrar Using PIN Method 37
     - 2.7.3 Example to Add to Registrar Using PBC Method 40
     - 2.7.4 Example to Configure a Network/AP Using PIN or PBC Method 44
3. Security 46
   - 3.1 Auth.\ Encry. Setting – WEP/TKIP/AES 46
   - 3.2 802.1x Setting 47
   - 3.3 Example to Configure Connection with WEP on 50
   - 3.4 Example to Configure Connection with WPA-PSK 52
   - 3.5 Example to Configure Connection with WPA 54
4. Appendix 59
   - 4.1 Country Channel List 59
   - 4.2 Acknowledgements 61
5. FAQ 62
   - 5.1 FAQ 62

1. Windows Wireless Utility

1.1 Windows Zero Configuration for XP

1.1.1 Ralink Wireless Utility and Windows Zero Configuration

Windows XP includes a wireless configuration utility named "Windows Zero configuration" (WZC) which provides basic configuration functions to the Ralink Wireless NIC. Ralink's utility (RaUI) additionally provides WPA functionality. To make it easier for the user to select the correct utility. RaUI will let users make a selection when it first runs after windows XP boots.

Right-clicking the icon will bring up the selection window and allow the user to make a selection.

Figure 1-1 RaUI.exe

RaUI can co-exist with WZC. When coexisting with WZC, RaUI only provides monitoring functions, such as surveying the link status, network status, statistic counters, advanced feature status, WMM status and WPS status. It won't interfere with WZC's configuration or profile functions. It is shown as Figure 1-2.

Figure 1-2 Select WZC or RaUI

If "Use RaConfig as Configuration utility" is selected, please jump to Section 2 on running RaUI.

If "Use Zero Configuration as Configuration utility" is selected, please continue.

We will explain the difference between RaUI and WZC. Figure 1-3 shows the RaUI status when WZC is activated as the main control utility.

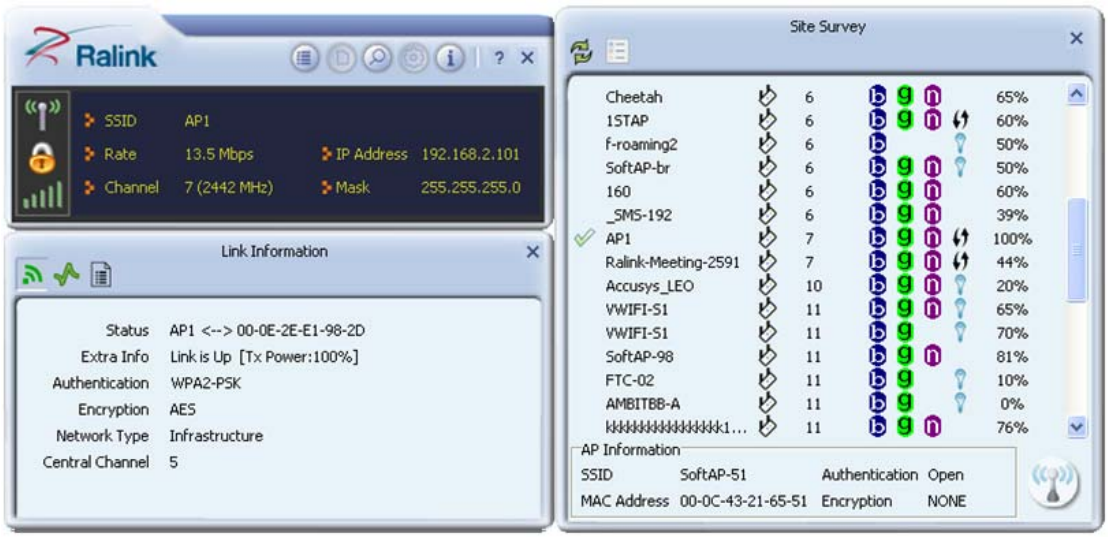


Figure 1-3 RaUI status with WZC active

When activating WZC, there are several difference with the RaUI status, compared to the RaUI status without WZC running.

- The profile button will be gray. Profile functionality is removed since the NIC is controlled by WZC.
- The Connect and Add Profile function will be gray. Profile functionality is removed since the NIC is controlled by WZC.

Please read through this document for full details on the other functions provided by RaUI.

1.1.2 Windows Zero Configuration (WZC)

- If there is no connection or it is lost, the status prompt will pop up, as shown in Figure 1-4.

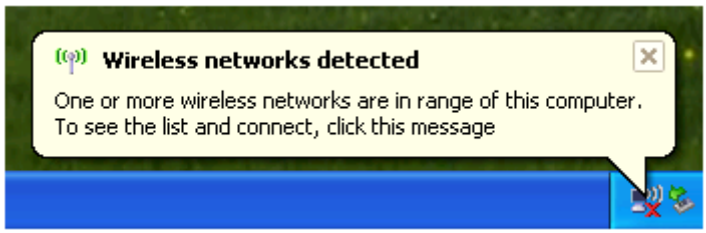

Wireless networks detected
One or more wireless networks are in range of this computer.
To see the list and connect, click this message

Figure 1-4 status prompt for no connection

- Right-click the network connection icon in taskbar.

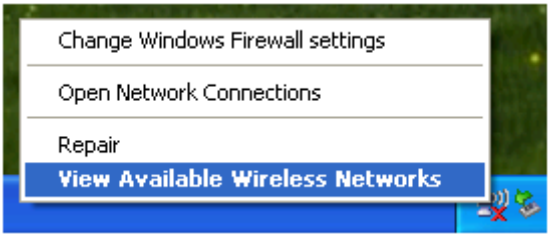


Figure 1-5 Select WZC main status

- Select "View Available Wireless Networks" and the "Wireless Network Connection" dialog box will pop up, as shown in Figure 1-6.

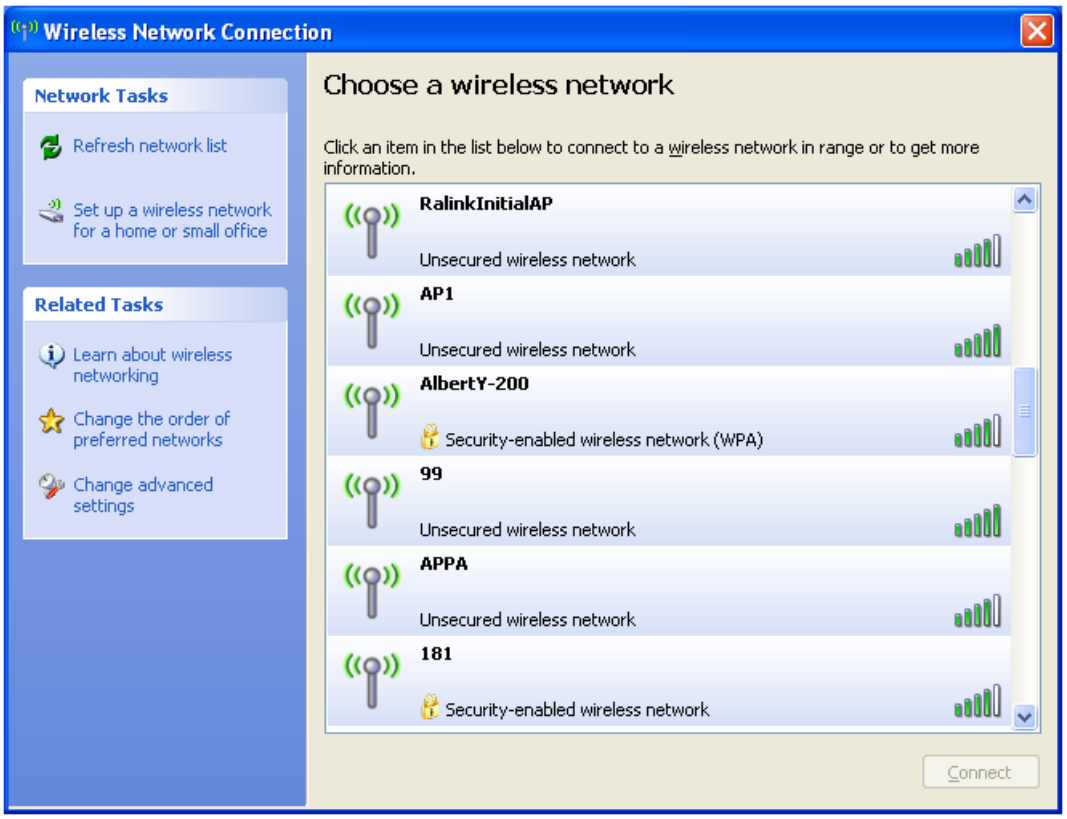


Figure 1-6 Wireless Network Connection

- Select the intended access point and click "Connect". Then click "Connect Anyway" as shown as Figure 1-7.

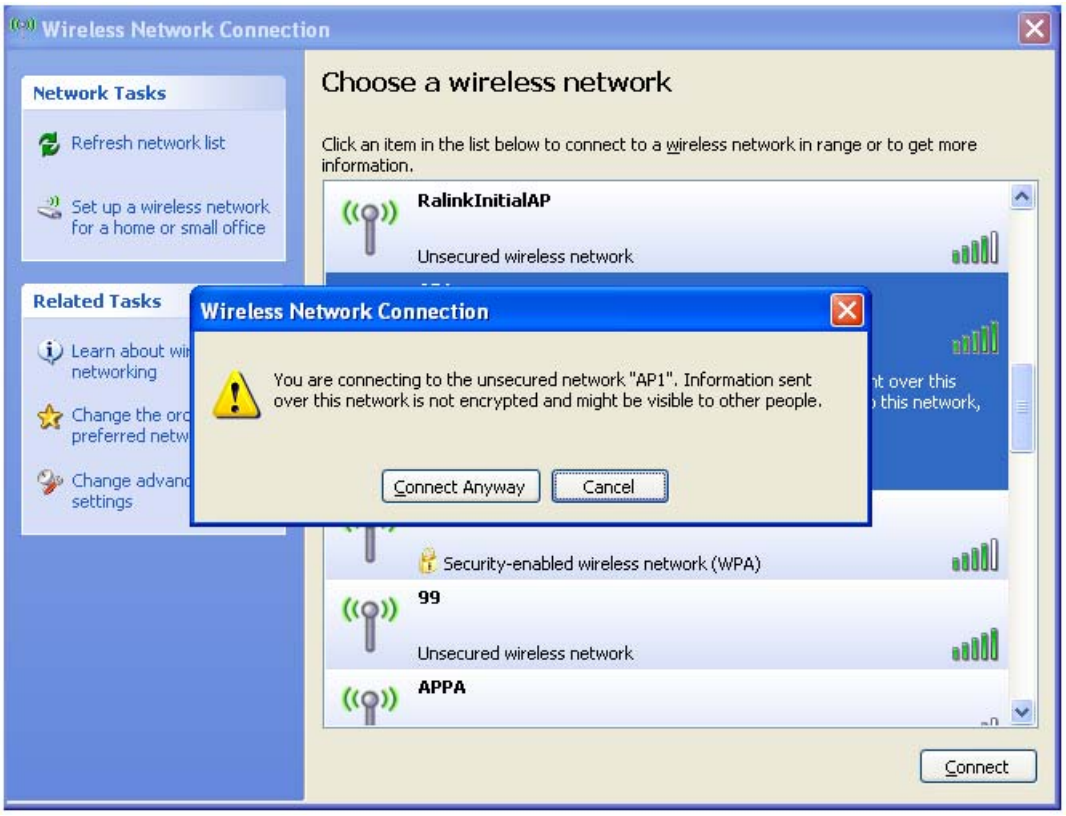

Wireless Network Connection
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Choose a wireless network
Click an item in the list below to connect to a wireless network in range or to get more information.
RalinkInitialAP
Unsecured wireless network
Wireless Network Connection
You are connecting to the unsecured network "AP1". Information sent over this network is not encrypted and might be visible to other people.
Connect Anyway
Cancel
Security-enabled wireless network (WPA)
99
Unsecured wireless network
APPA
Connect

Figure 1-7 Select intended AP: AP1, then click "Connect"

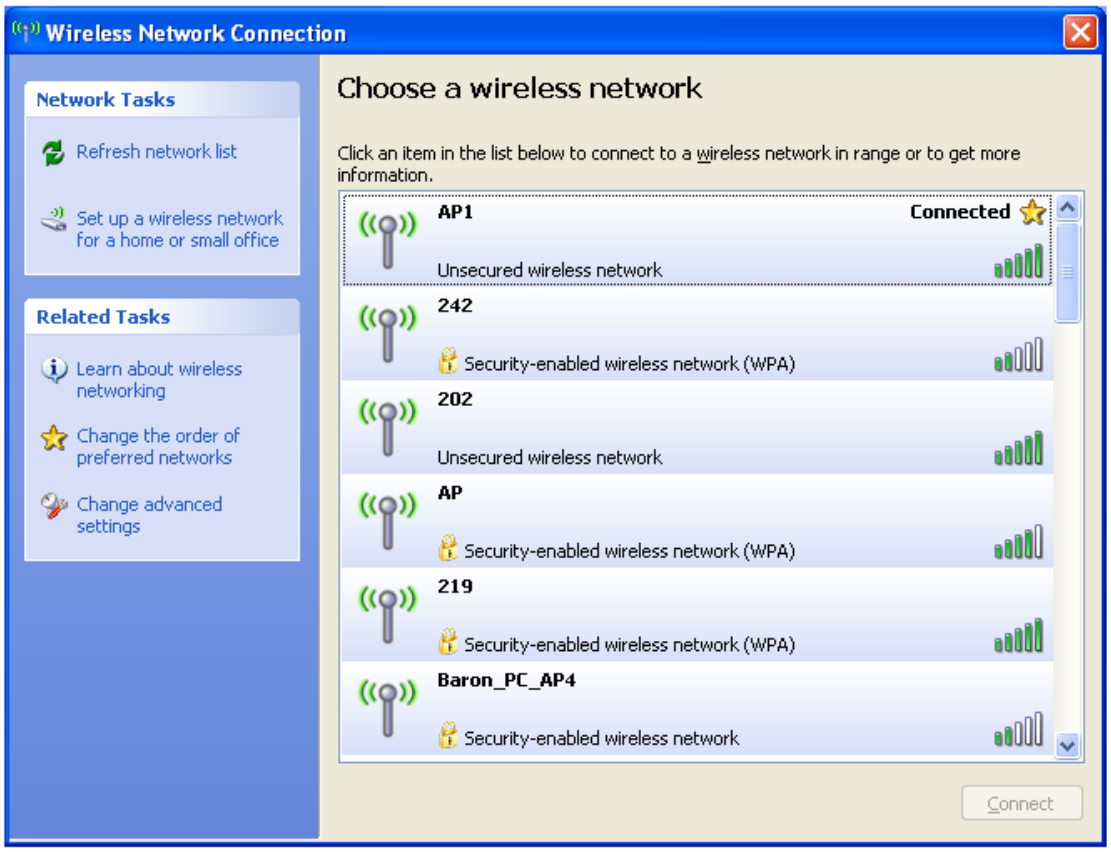


Figure 1-8 Connect AP: AP1 successfully

- If you want to modify information about the AP, click "Change advanced settings" as shown in Figure 1-9. Then select the "Wireless Networks" tab shown as Figure 1-10.

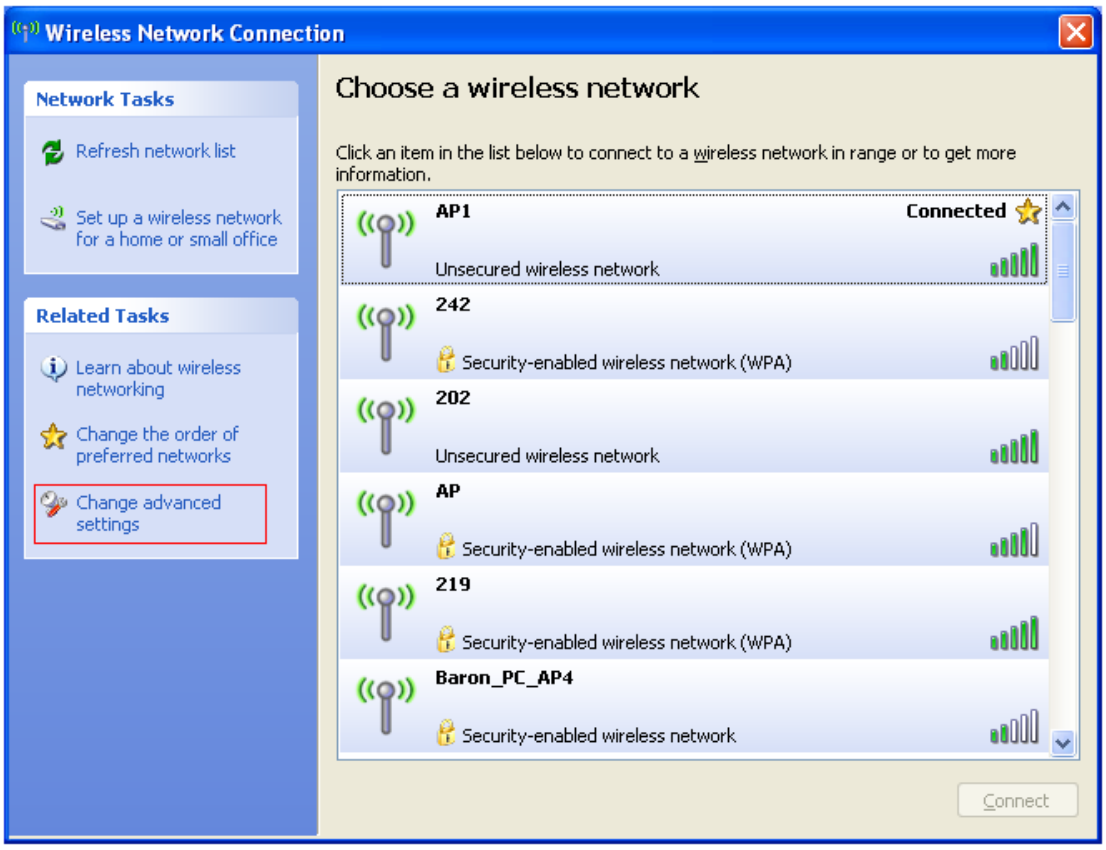


Figure 1-9 Click "Change advanced settings"

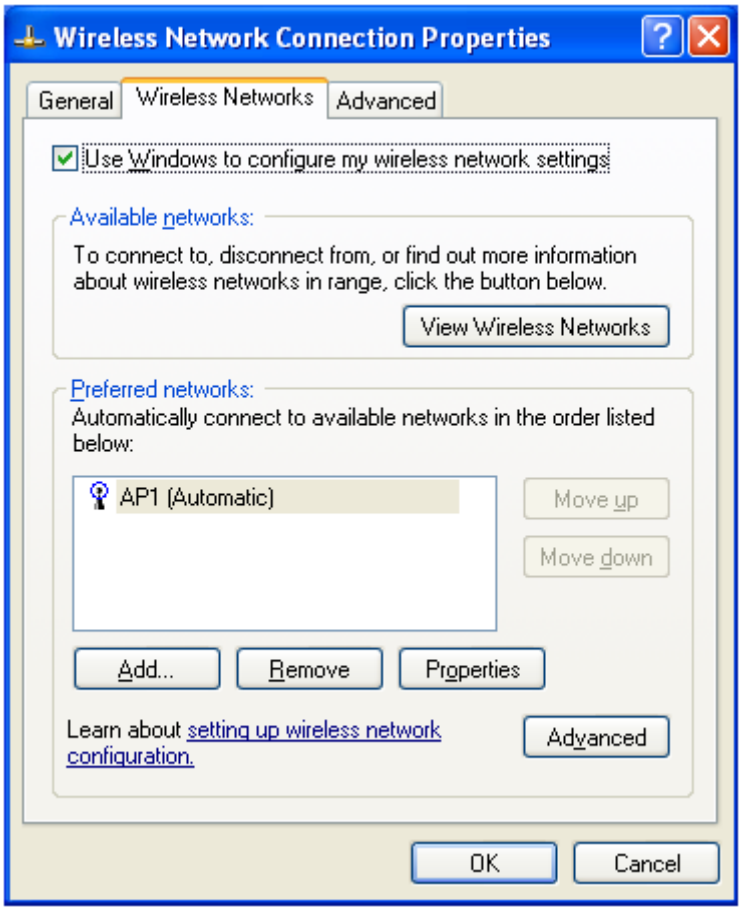


Figure 1-10 Choose the "Wireless Networks" tab

- Click "Properties" as shown in Figure 1-11. Then click "OK" button.

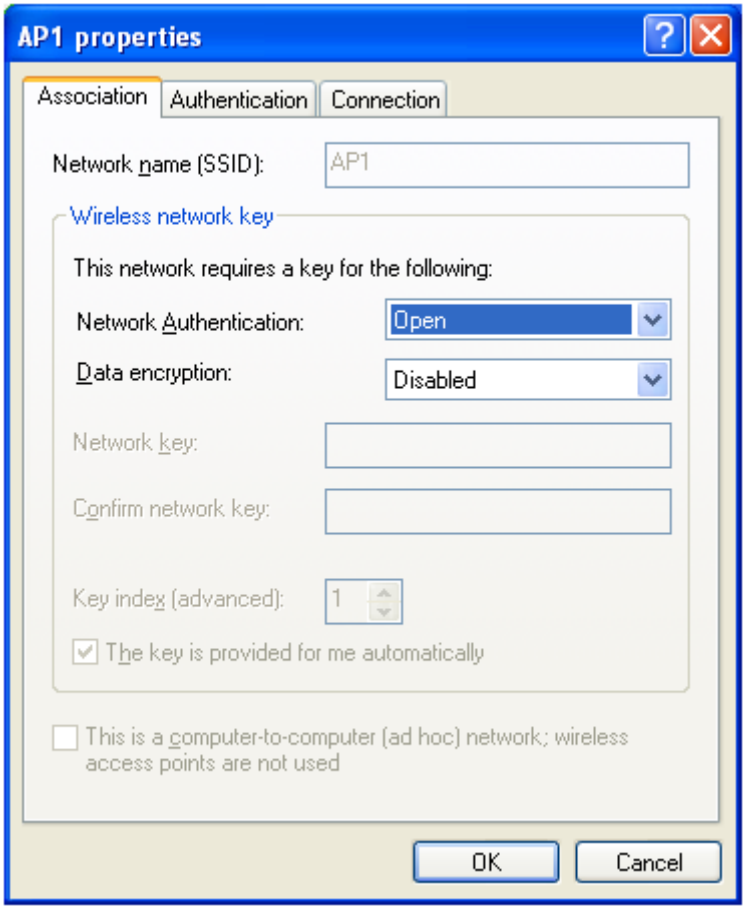


Figure 1-11 AP's properties

- After filling in the appropriate value, click "OK." The pop-up will indicate the status as shown in Figure 1-12.

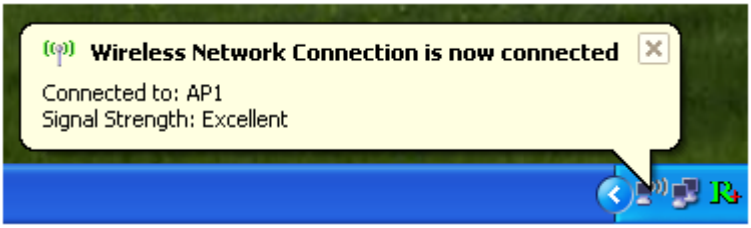


Figure 1-12 Network connection status

- Clicking the Ralink icon will bring up the RaUI main window. Users can find the surrounding APs in the list. The currently connected AP will be shown with a blue icon beside it, as shown in Figure 1-13. Users may use the advanced tab to configure more advanced features provided by Ralink's wireless NIC. For details on configuring the advanced features, please check the Advance setting section.

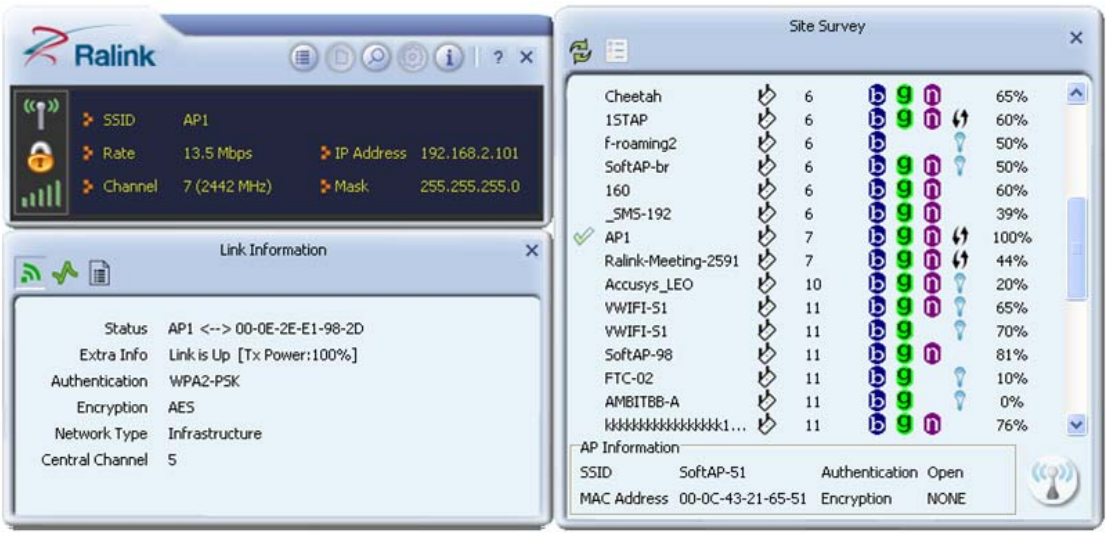


Figure 1-13 Show connection status by using WZC to initiate the connection

1.2 Windows AutoConfig Service for Vista

1.2.1 Ralink Wireless Utility and Windows AutoConfig Service

In Windows Vista, the Auto Config service provides basic wireless configuration functions for the Ralink Wireless Network Interface Controller. In order to perform these functions, the Auto Config service should first be enabled (Refer to Section 1-2-2).

Once the Ralink wireless utility is minimized, click the Ralink icon as shown in Figure 1-1. This will bring up the option menu shown as Figure 1-2 for the user to restore the utility window or terminate the utility.

Figure 1-1

Figure 1-2

The Ralink wireless utility as shown in Figure 1-3, provides profile management, the available networks listing, a statistical counter display, Wi-Fi multimedia (WMM), protected Wi-Fi setup, Cisco compatible extensions (CCX), call admission control (CAC), radio controls, Ralink driver/utility information, and help functions.

Figure 1-3 Ralink Utility

The Ralink wireless utility starts in compact mode as shown in Figure 1-3. Clicking the expanding icon at the bottom-right corner can change to the full mode as shown in Figure 1-4.

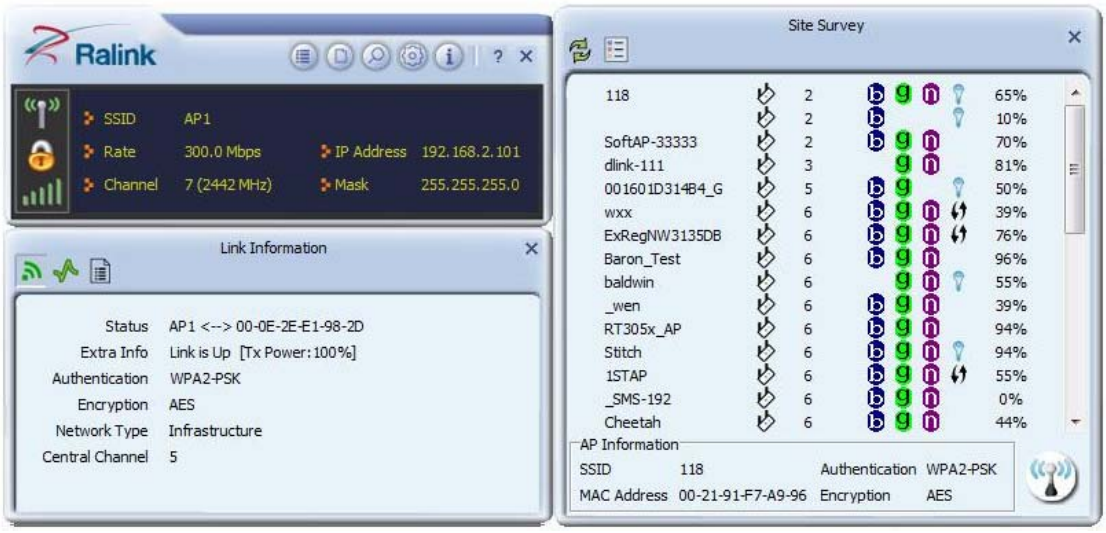
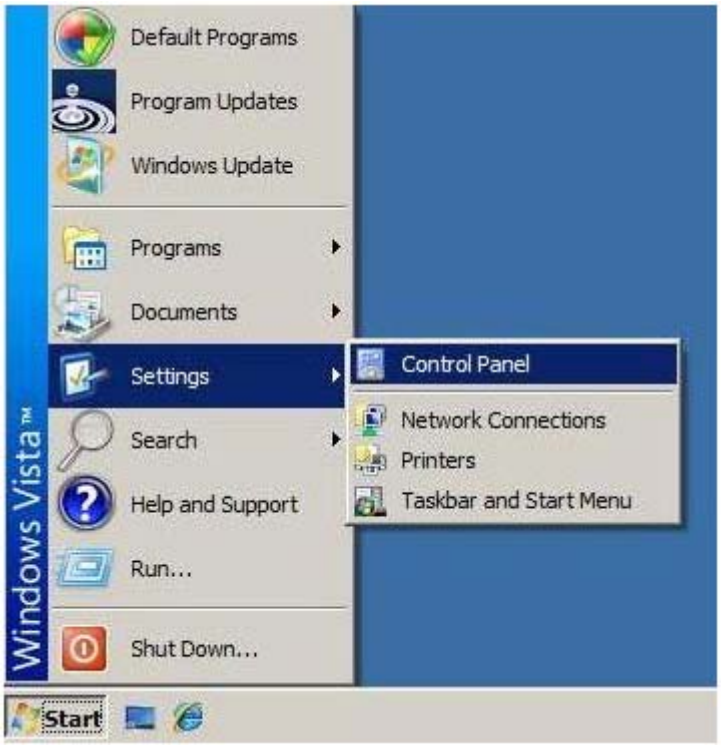


Figure 1-4 Ralink Utility in full mode

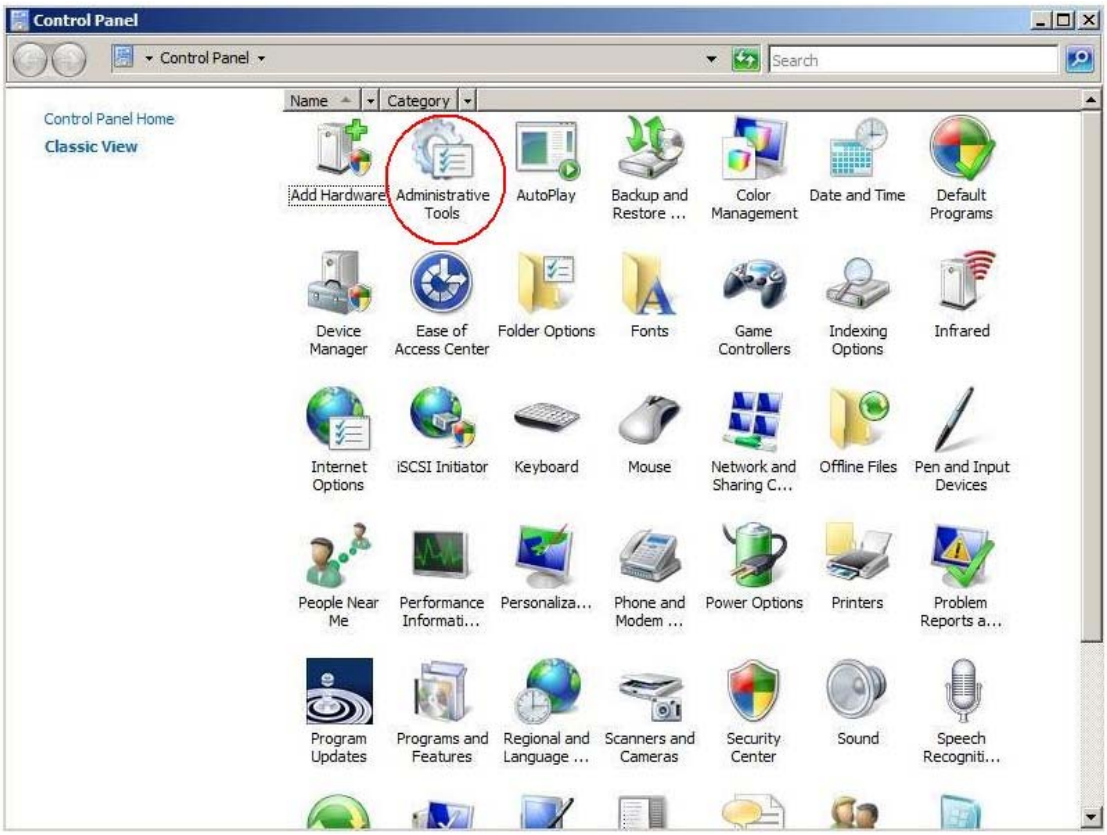
1.2.2 Windows AutoConfig Service

The following steps outline the procedure for starting/stopping the Windows AutoConfig service.

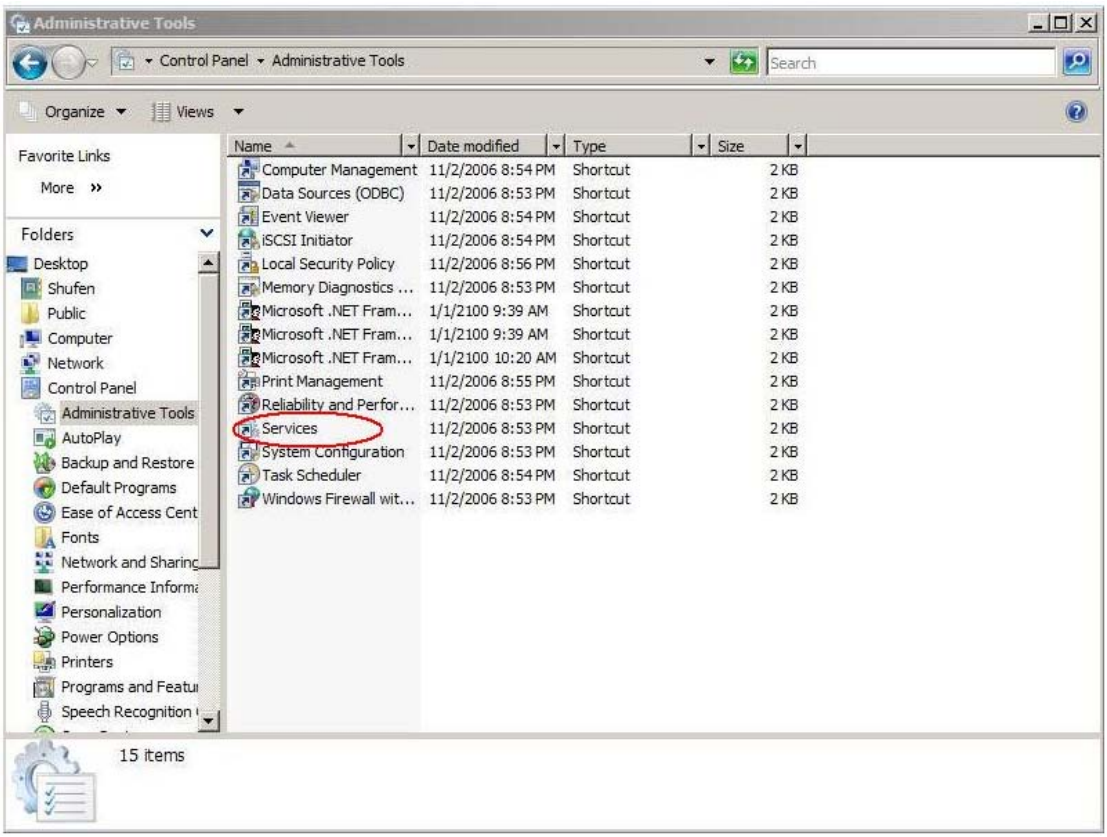
Select "Control Panel" from "Settings" in the start menu



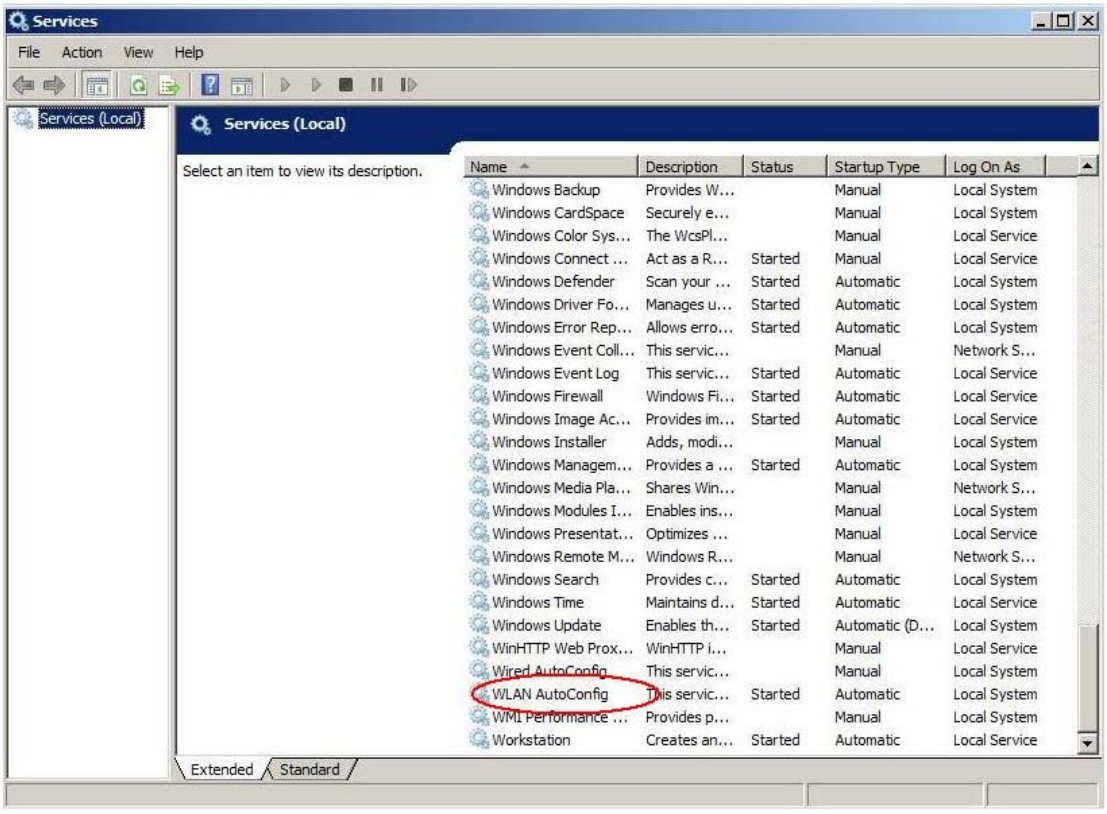
Double-click the "Administrative Tools" icon



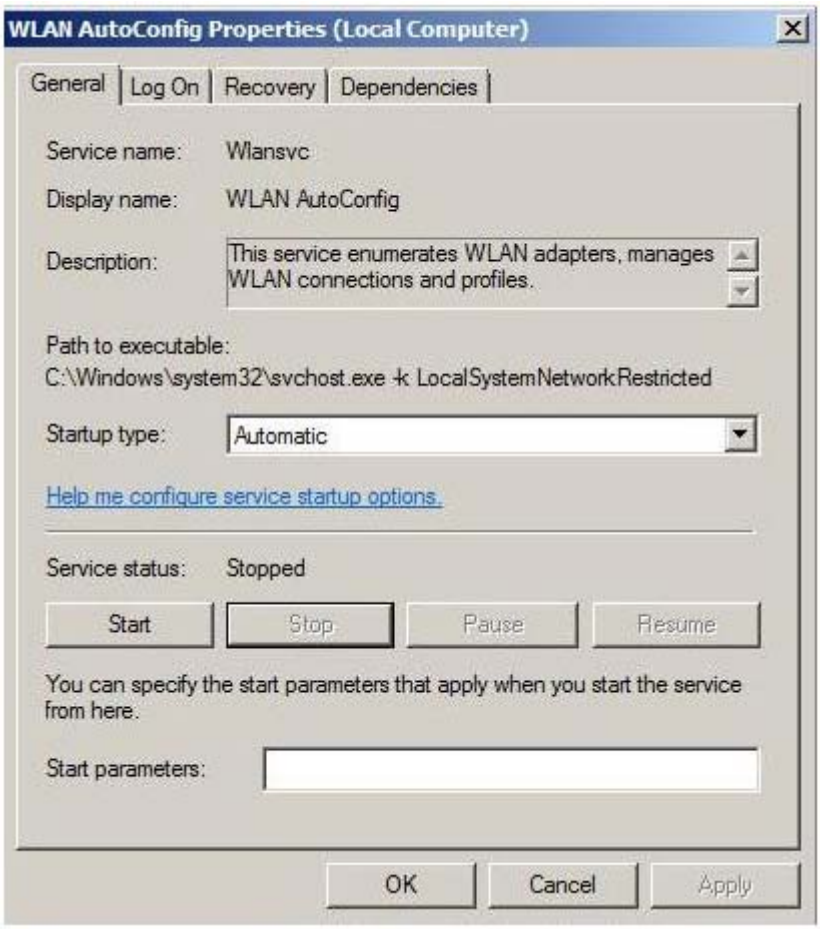
Double-click "Services"



Double-click "WLAN AutoConfig"


Services
File Action View Help
Services (Local)
Services (Local)
Select an item to view its description.
Name
Description
Status
Startup Type
Log On As
Windows Backup Provides W... Manual Local System
Windows CardSpace Securely e... Manual Local System
Windows Color Sys... The WcsPl... Manual Local Service
Windows Connect ... Act as a R... Started Manual Local Service
Windows Defender Scan your ... Started Automatic Local System
Windows Driver Fo... Manages u... Started Automatic Local System
Windows Error Rep... Allows erro... Started Automatic Local System
Windows Event Coll... This servic... Manual Network S...
Windows Event Log This servic... Started Automatic Local Service
Windows Firewall Windows Fi... Started Automatic Local Service
Windows Image Ac... Provides im... Started Automatic Local Service
Windows Installer Adds, modi... Manual Local System
Windows Managem... Provides a ... Started Automatic Local System
Windows Media Pla... Shares Win... Manual Network S...
Windows Modules I... Enables ins... Manual Local System
Windows Presentat... Optimizes ... Manual Local Service
Windows Remote M... Windows R... Manual Network S...
Windows Search Provides c... Started Automatic Local System
Windows Time Maintains d... Started Automatic Local Service
Windows Update Enables th... Started Automatic (D... Local System
WinHTTP Web Prox... WinHTTP i... Manual Local Service
Wired AutoConfig This servic... Manual Local System
WLAN AutoConfig This servic... Started Automatic Local System
WMI Performance ... Provides p... Manual Local System
Workstation Creates an... Started Automatic Local Service
Extended
Standard

Manage the AutoConfig properties in the dialog box

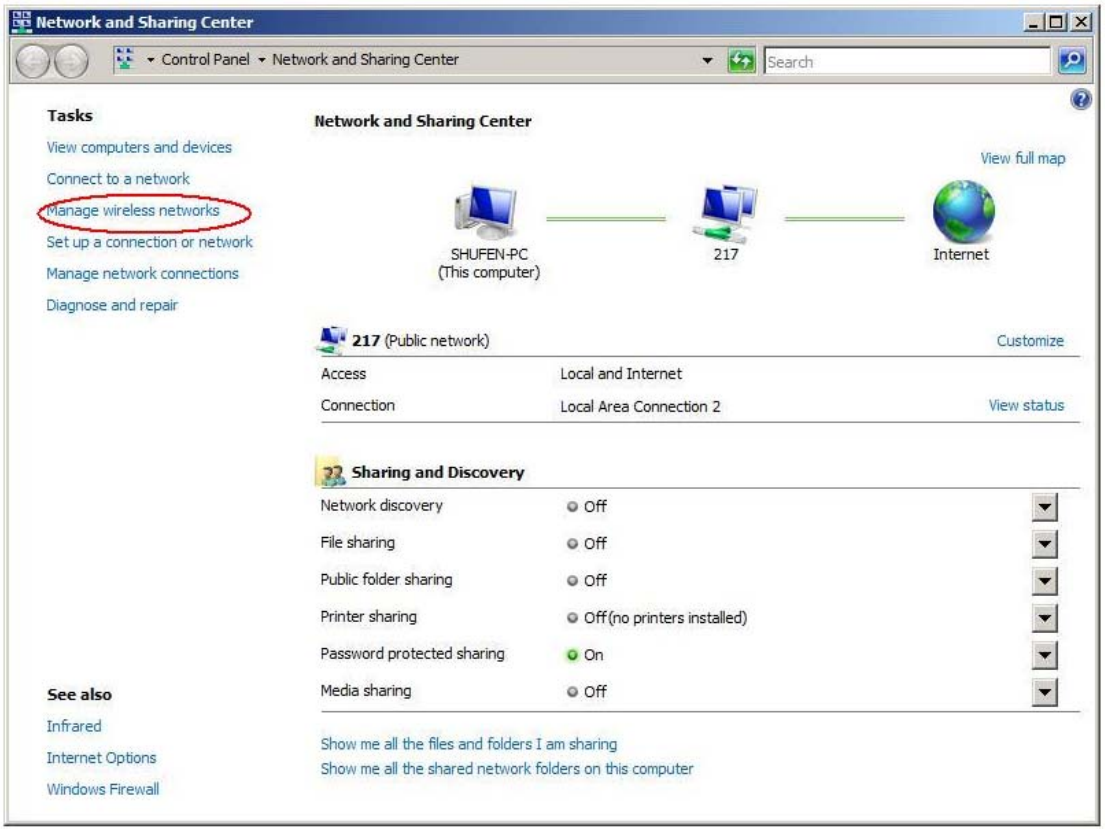


Windows profile manager can be accessed via control panel or network connection icon in the task bar.

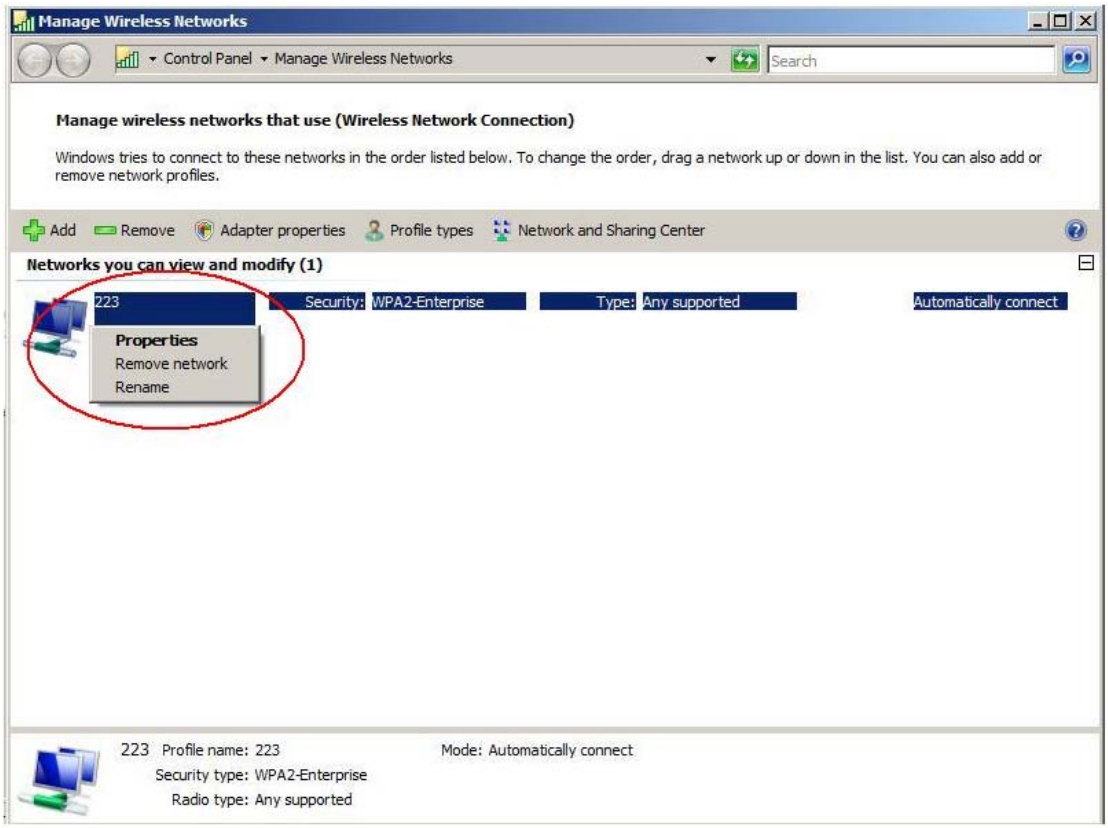
1. Access via network connection icon

Right-click the network connection icon in the taskbar, then select "Network and Sharing Center" from the pop-up menu

Select "Manage wireless networks" from the tasks list

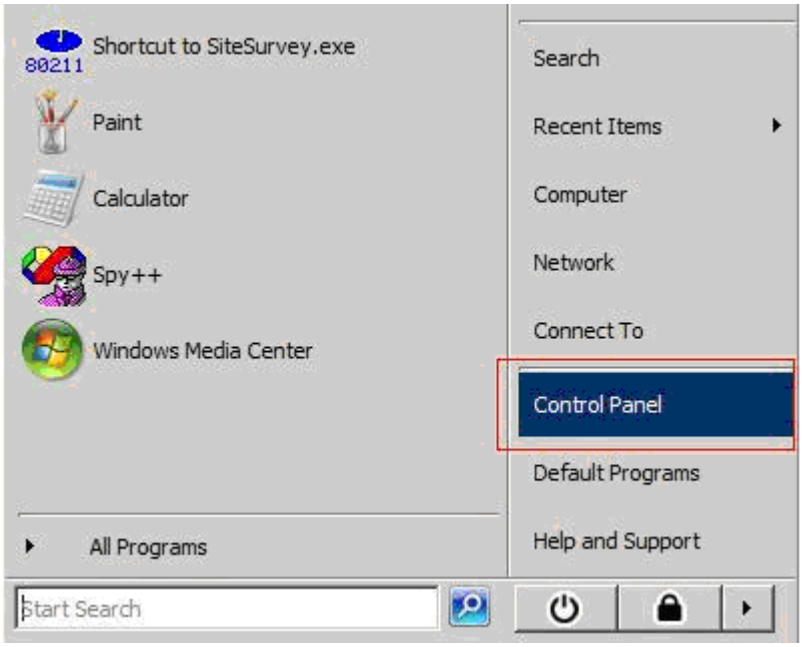


Right-click the network to bring up the profile managing menu

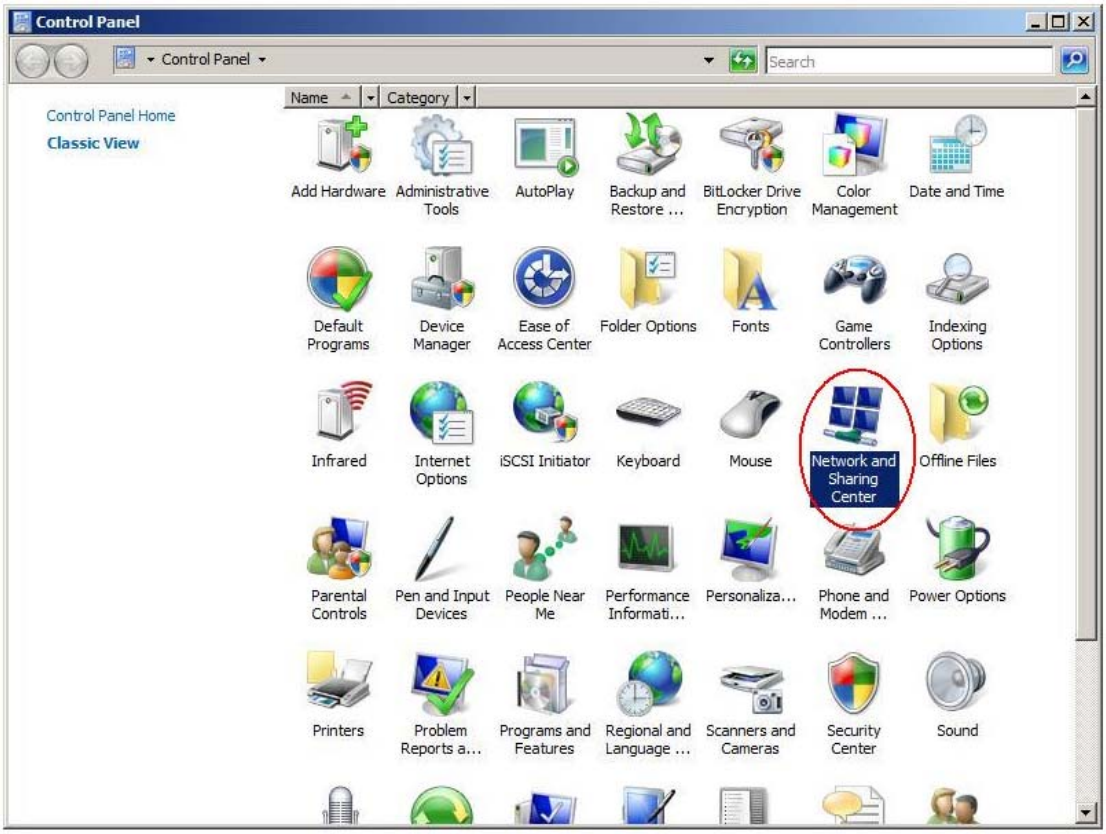

Manage Wireless Networks
Control Panel ▸ Manage Wireless Networks
Search
Manage wireless networks that use (Wireless Network Connection)
Windows tries to connect to these networks in the order listed below. To change the order, drag a network up or down in the list. You can also add or remove network profiles.
Add
Remove
Adapter properties
Profile types
Network and Sharing Center
Networks you can view and modify (1)
223
Security: WPA2-Enterprise
Type: Any supported
Automatically connect
Properties
Remove network
Rename
223 Profile name: 223
Security type: WPA2-Enterprise
Radio type: Any supported
Mode: Automatically connect

2. Access via control panel

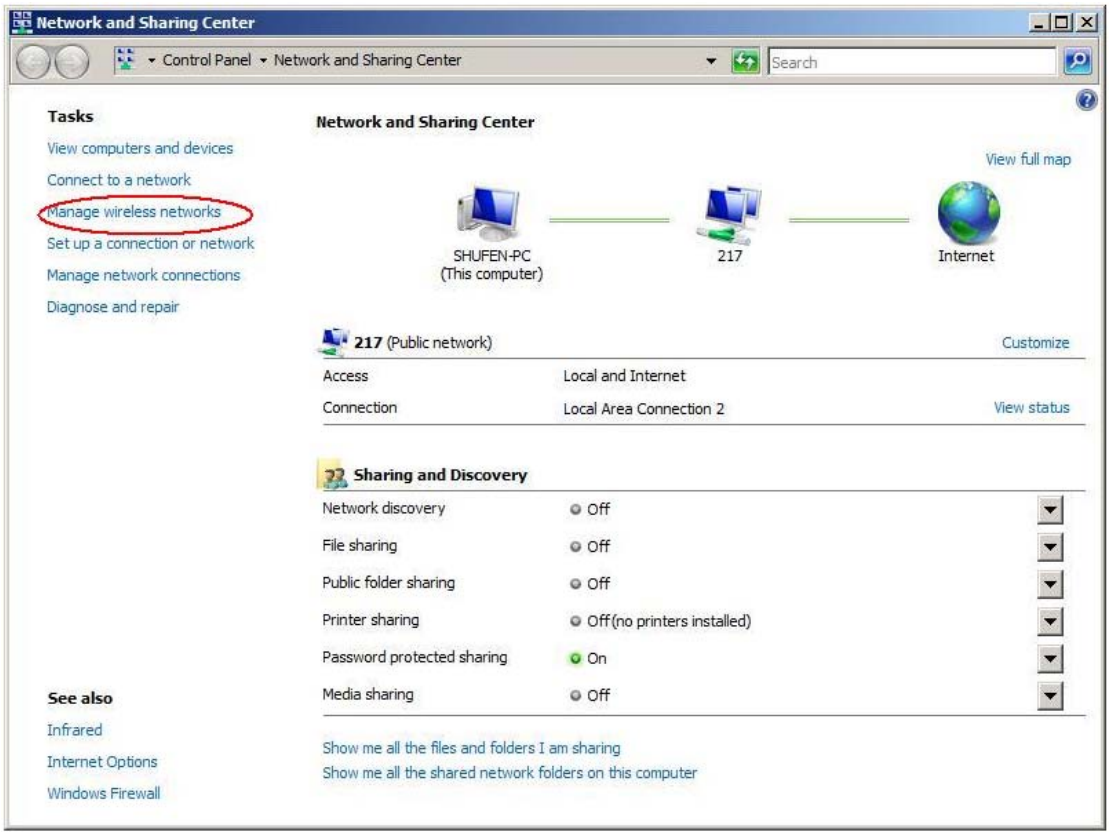
Select "Control Panel" from the start menu



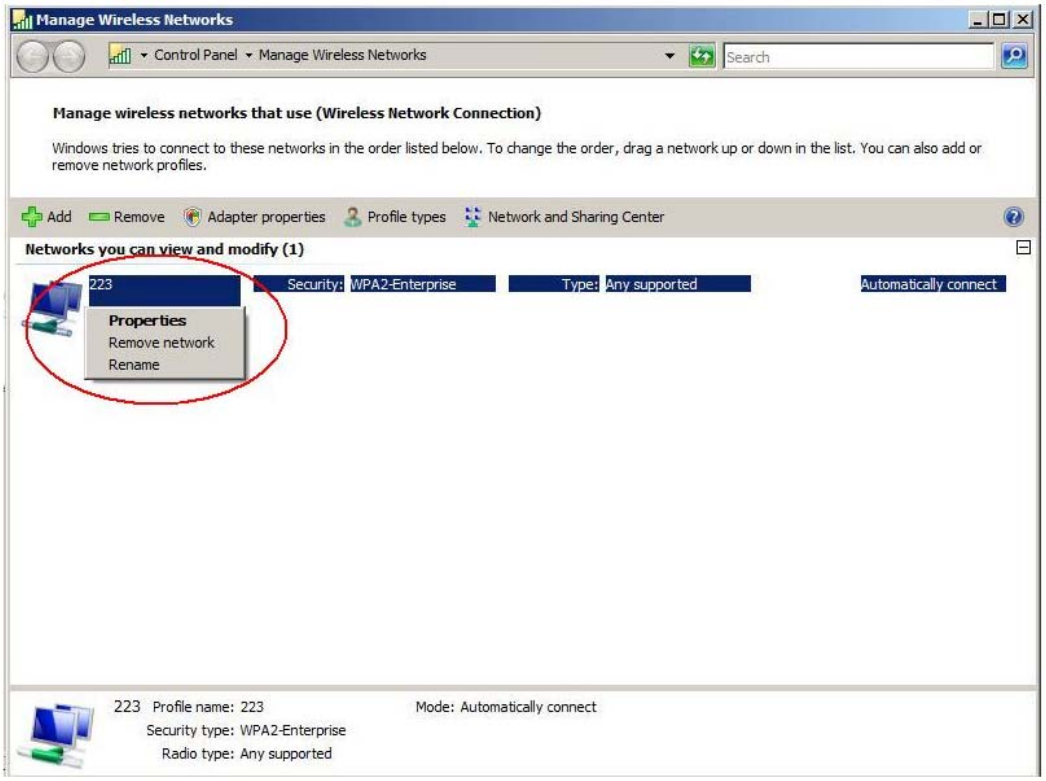
Double-click the "Network and Sharing Center" icon



Select "Manage wireless networks" from the tasks list



Right-click the network to bring up the profile managing menu


Manage Wireless Networks
Control Panel ▸ Manage Wireless Networks
Search
Manage wireless networks that use (Wireless Network Connection)
Windows tries to connect to these networks in the order listed below. To change the order, drag a network up or down in the list. You can also add or remove network profiles.
Add
Remove
Adapter properties
Profile types
Network and Sharing Center
Networks you can view and modify (1)
223
Security: WPA2-Enterprise
Type: Any supported
Automatically connect
Properties
Remove network
Rename
223 Profile name: 223
Security type: WPA2-Enterprise
Radio type: Any supported
Mode: Automatically connect

2. Ralink Wireless Utility (RaUI)

2.1 Start

2.1.1 Start RaUI

When starting RaUI, the system will connect to the AP with best signal strength without setting a profile or matching a profile setting. When starting RaUI, it will issue a scan command to a wireless NIC. After two seconds, the AP list will be updated with the results of a BSS list scan. The AP list includes most used fields, such as SSID, network type, channel used, wireless mode, security status and the signal percentage. The arrow icon indicates the connected BSS or IBSS network. The dialog box is shown in Figure 2-1.

Figure 2-1-1 RaUI section introduction

There are three sections to the RaUI dialog box. These sections are briefly described as follow.

Button Section: Include buttons for selecting the Profile page, Network page, Advanced page, Statistics page, WMM page, WPS page, the About button, Radio On/Off button and Help.

Figure 2-1-2 Button section

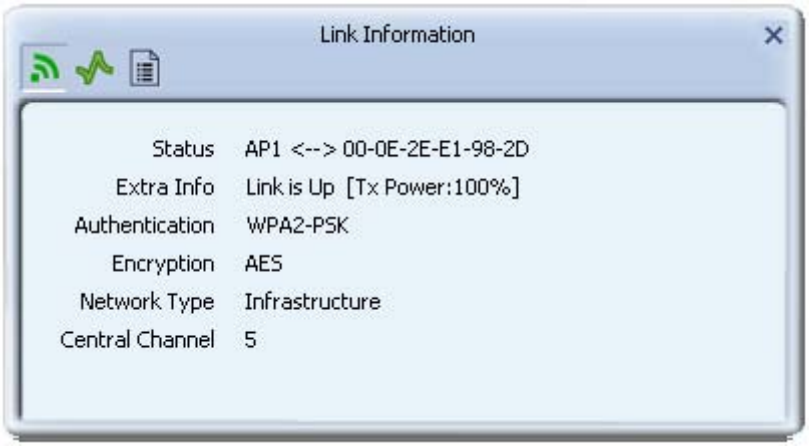


Figure 2-1-3 Link Information page

Figure 2-1-4 Profile page

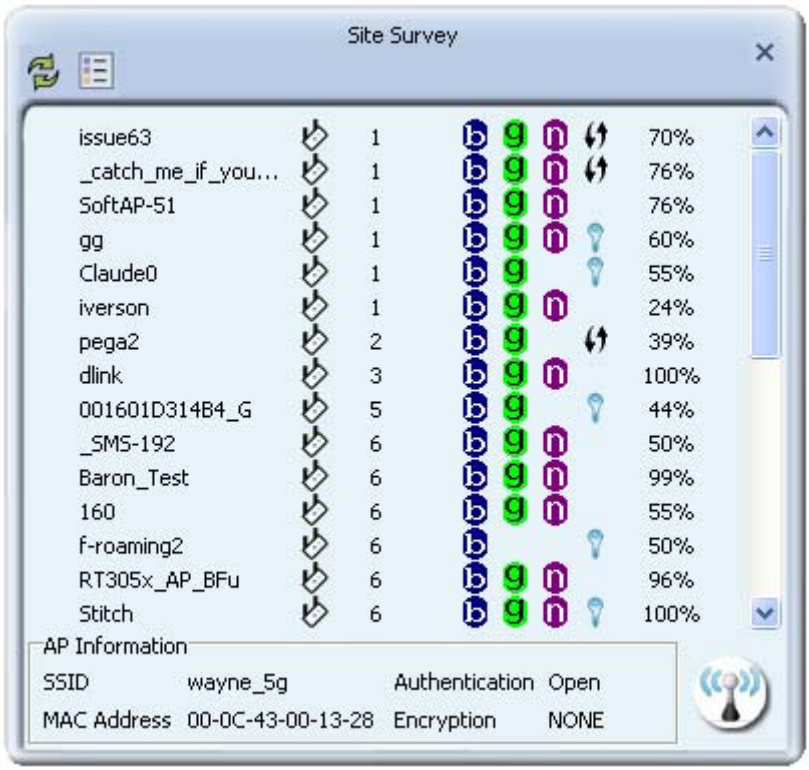


Figure 2-1-5 Network page

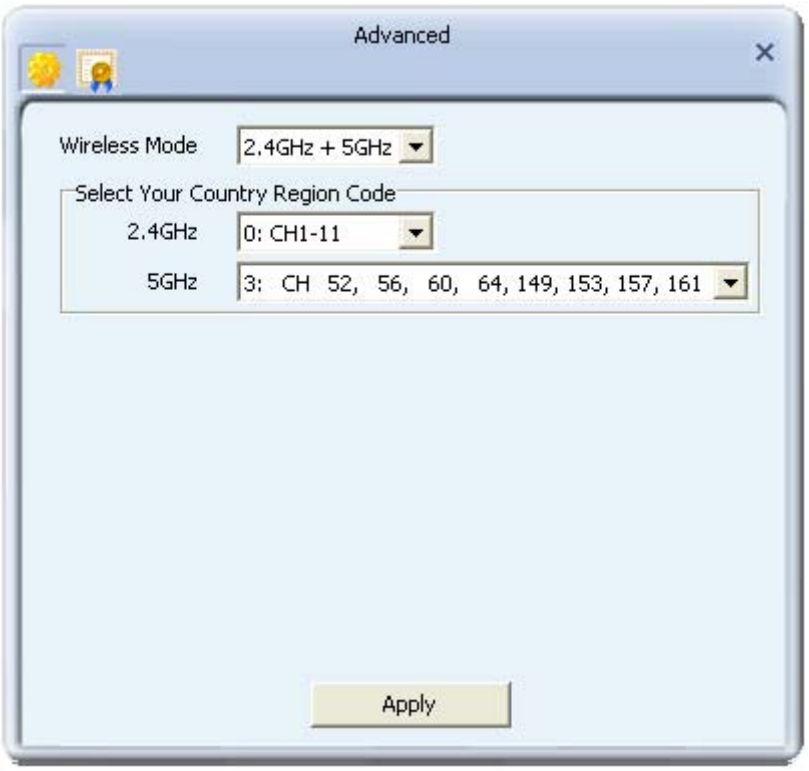


Figure 2-1-6 Advance page

Figure 2-1-7 About page

When starting RaUI, a small Ralink icon appears in the notifications area of the taskbar, as shown in Figure 2-1-15. You can double click it to maximize the dialog box if you selected to close it earlier. You may also use the mouse's right button to close RaUI utility.

Figure 2-1-8 Ralink icon in system tray

Additionally, the small icon will change color to reflect current wireless network connection status. The status is shown as follows:

: Indicates the connected and signal strength is good.

: Indicates the connected and signal strength is normal.

: Indicates that it is not yet connected.

: Indicates that a wireless NIC can not be detected.

: Indicates that the connection and signal strength is weak.

2.2 Profile

2.2.1 Profile

The Profile List keeps a record of your favorite wireless settings at home, office, and other public hot-spots. You can save multiple profiles, and activate the correct one at your preference. Figure 2-2-1 shows the basic profile section.

Figure 2-2-1 Profile function

Definition of each field:

- Profile Name: Name of profile, preset to PROF* (* indicate 1, 2, 3...).
- SSID: The access point or Ad-hoc name.
- Network Type: Indicates the networks type, including infrastructure and Ad-Hoc.
- Authentication: Indicates the authentication mode used.
- Encryption: Indicates the encryption Type used.
- Use 802.1x: Shows if the 802.1x feature is used or not.
- Cannel: Channel in use for Ad-Hoc mode.
- Power Save Mode: Choose from CAM (Constantly Awake Mode) or Power Saving Mode.
- Tx Power: Transmitting power, the amount of power used by a radio transceiver to send the signal out.
- RTS Threshold: Users can adjust the RTS threshold number by sliding the bar or keying in the value directly.

- Fragment Threshold: The user can adjust the Fragment threshold number by sliding the bar or key in the value directly.

Icons and buttons:

: Indicates if a connection made from the currently activated profile.

: Indicates if the connection has failed on a currently activated profile.

: Indicates the network type is infrastructure mode.

: Indicates the network type is in Ad-hoc mode.

: Indicates if the network is security-enabled.

: Click to add a new profile.

: Click to edit an existing profile.

: Deletes an existing profile.

: Import an existing profile.

: Export an existing profile.

: Activates the selected profile.

2.2.2 Add/Edit Profile

There are three methods to open the Profile Editor dialog box.
You can open it by clicking the "Add to Profile" button in the Site Survey tab.
You can open it by clicking the "Add" button in the Profile tab.
You can open it by clicking the "Edit" button on the Profile tab.

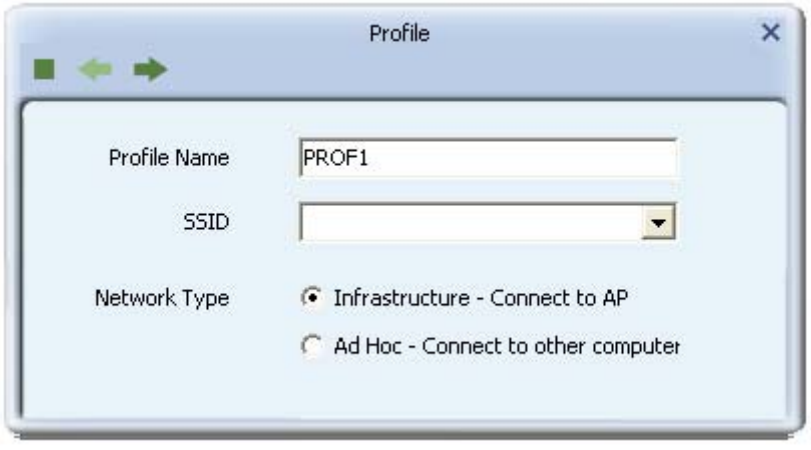


Figure 2-2-1 Add a new Profile

Icons and buttons:

- : To the next page.
- : Back to the previous page.
- : Cancel button.

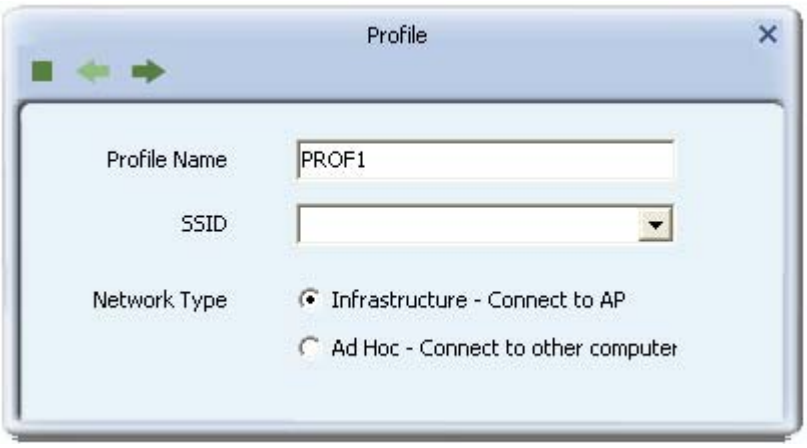


Figure 2-2-2 Profile Name, SSID, Network Configuration

- Profile Name: The user can chose any name for this profile, or use the default name defined by system.
- SSID: The user can key in the intended SSID name or select one of the available APs from the drop-down list.
- Power Save Mode: Choose CAM (Constantly Awake Mode) or Power Saving Mode.
- Network Type: There are two types, infrastructure and 802.11 Ad-hoc modes. Under Ad-hoc mode, user can also choose the preamble type. The available preamble type includes auto and long. In addition, the channel field will be available for setup in Ad-hoc mode.

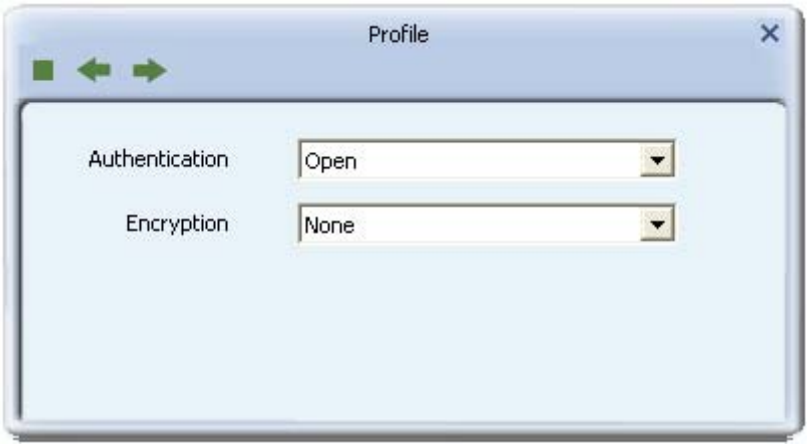


Figure 2-2-3 Authentication and Encryption Configuration

- Authentication Type: There are 7 types of authentication modes supported by RaUI. They are open, Shared, LEAP, WPA and WPA-PSK, WPA2 and WPA2-PSK, 802.1X, WAPI-PSK, and WAPI-CA.
- Encryption Type: For open and shared authentication mode, the selection of available encryption type are none and WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode, both TKIP and AES encryption is available.

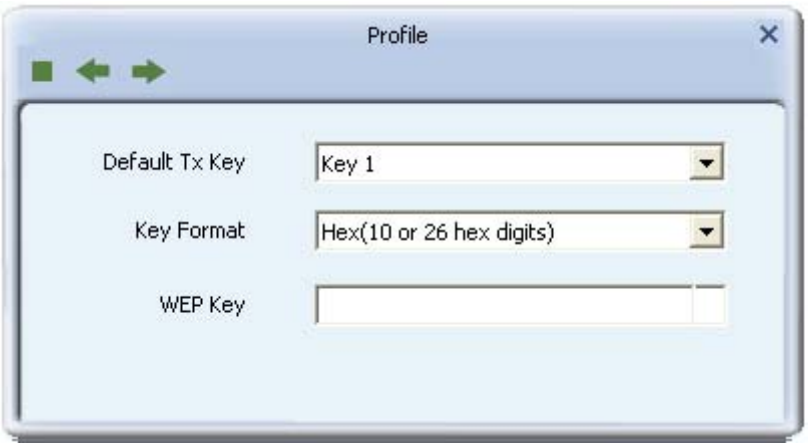


Figure 2-2-4 WEP Key Configuration

- WEP Key: Only valid when using WEP encryption algorithms. The key must be identical to the AP's key. There are several formats to enter the keys.

1. Hexadecimal - 40bits: 10 Hex characters.
2. Hexadecimal - 128bits: 26 Hex characters.
3. ASCII - 40bits: 5 ASCII characters.
4. ASCII - 128bits: 13 ASCII characters.

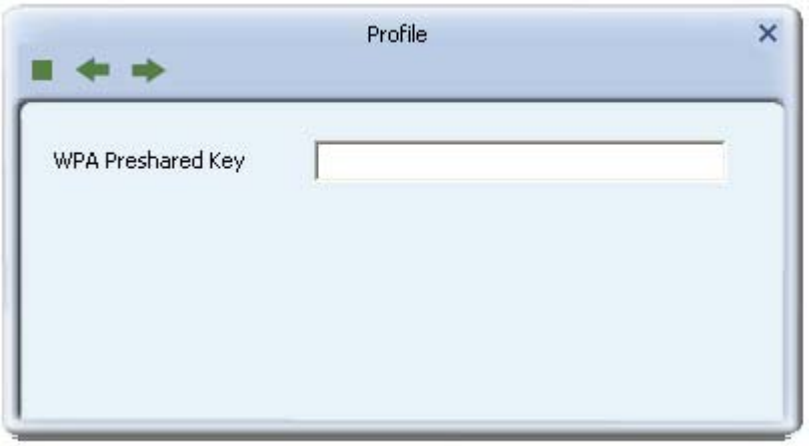


Figure 2-2-5 Pre-shared Key Configuration

- Pre-shared Key: This is the key shared between the AP and STA. For WPA-PSK and WPA2-PSK authentication mode, this field must be filled with a key between 8 and 32 characters in length.

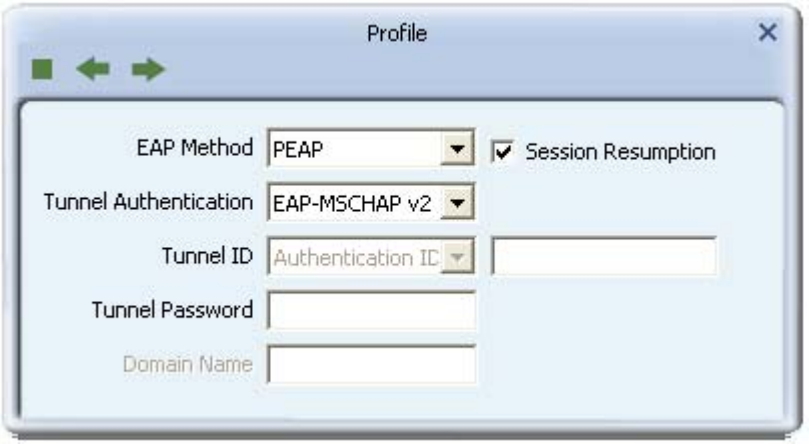


Figure 2-2-6 802.1x Configuration

- 802.1x Setting: This is introduced in the topic of “Section 3-2 : 802.1x Setting”

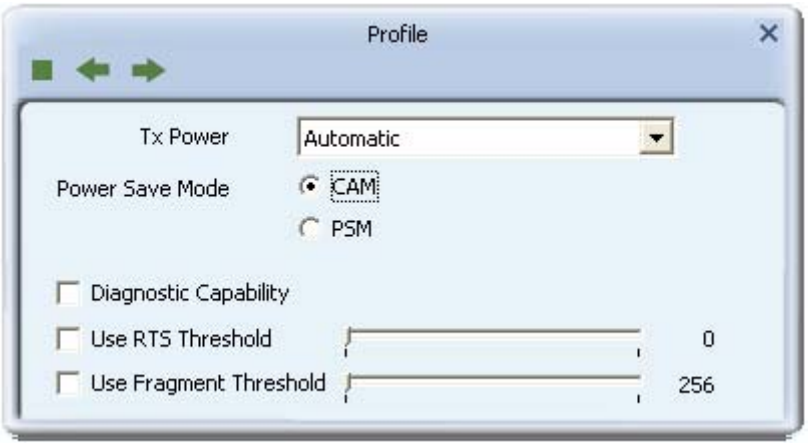


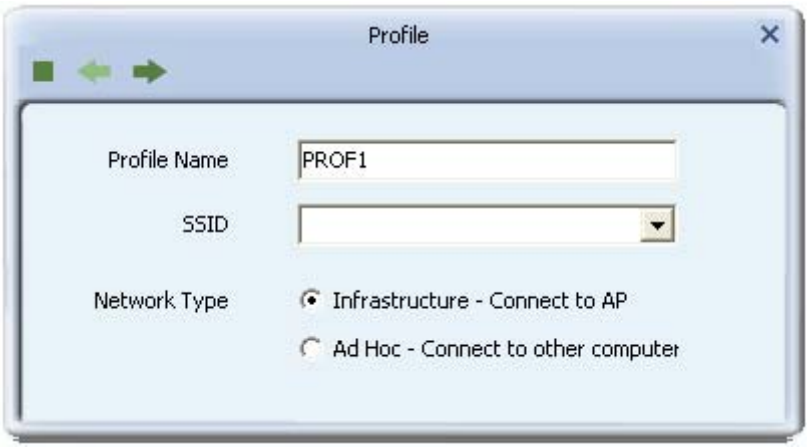
Figure 2-2-7 Advanced Configuration

- Power Save Mode: Choose CAM (Constantly Awake Mode) or Power Saving Mode.
- Channel: Only available for setting under Ad-hoc mode. Users can choose the channel frequency to start their Ad-Hoc network.
- RTS Threshold: User can adjust the RTS threshold number by sliding the bar, or key in the value directly. The default value is 2347.
- Fragment Threshold: User can adjust the Fragment threshold number by sliding the bar or key in the value directly. The default value is 2346.

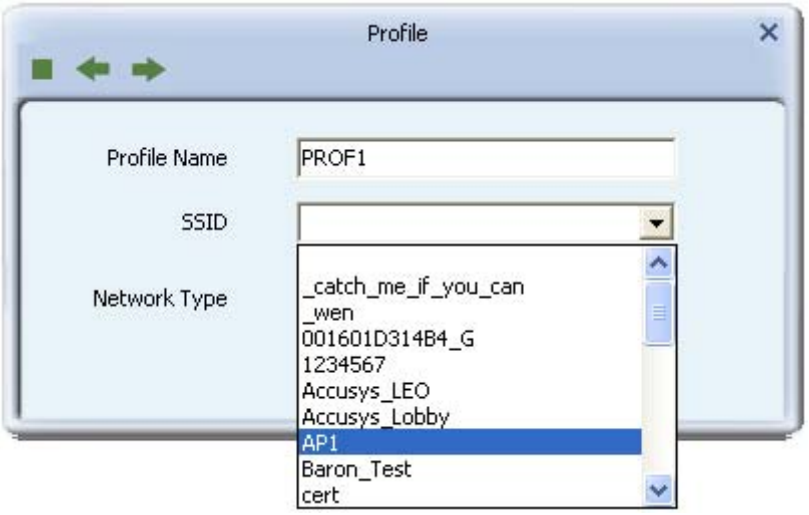
2.2.3 Example to Add Profile in Profile

- Click "Add" below the Profile List.

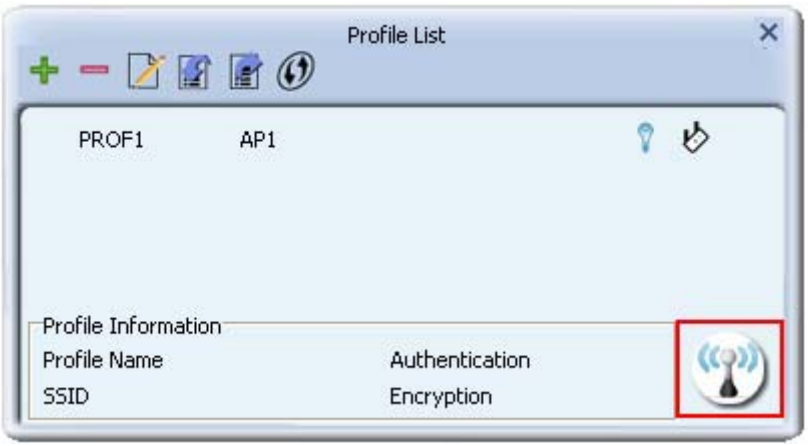
- The "Add Profile" will appear.



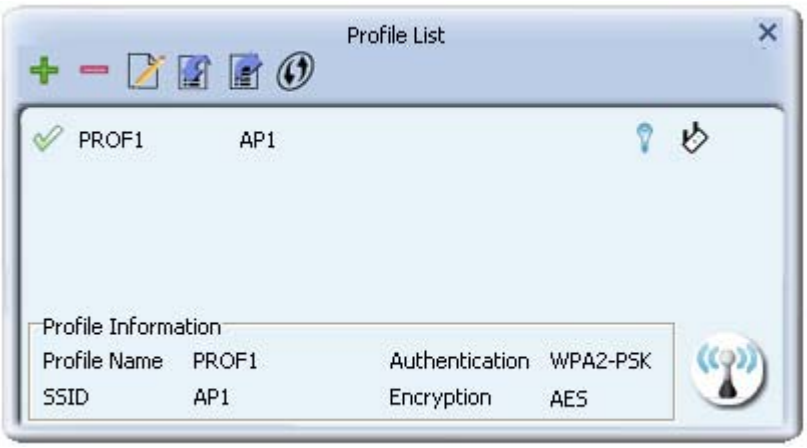
- Specify a Profile Name. Select an AP from the SSID drop-down list. The AP list from the last Network.



- Now the profile which the user set appears in the profile list. Click "Activate".



- Now the profile which the user active will connect to AP.



2.2.4 Pre-logon Connect

The Pre-logon Connect configuration page as shown in Figure 2-2-4.

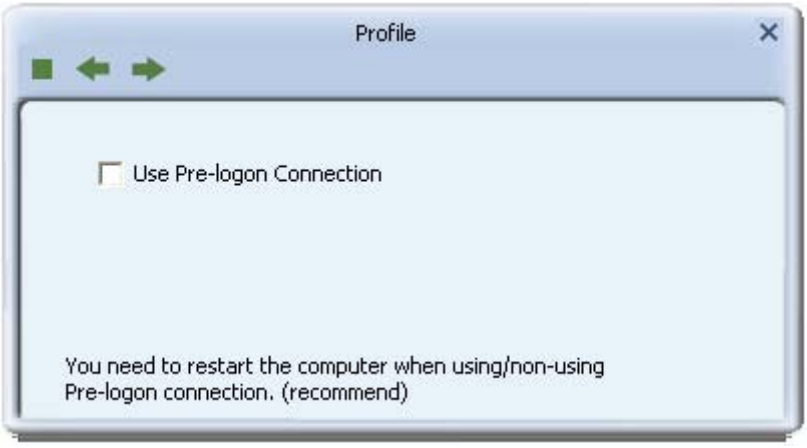


Figure 2-2-4 Pre-logon Connect Page

Field definitions:

- Pre-logon Connect: Use ID and Password in Profile.

** Recommend: You need to restart the computer when using/non-using Pre-logon connection.

2.3 Network

2.3.1 Network

The system will display the information of local APs from the last scan result as part of the Network section. The Listed information includes the SSID, BSSID, Signal, Channel, Encryption algorithm, Authentication and Network type as shown in Figure 2-3-1-1.

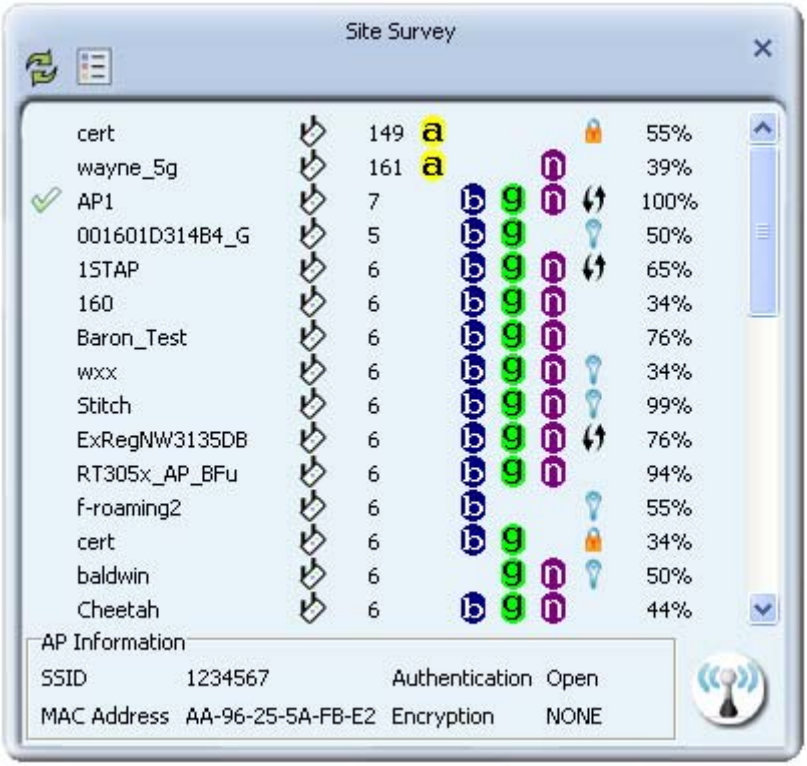


Figure 2-3-1-1 Network function

Definition of each field:

- SSID: Name of BSS or IBSS network.
- Network Type: Network type in use, Infrastructure for BSS, Ad-Hoc for IBSS network
- Channel: Channel in use.
- Wireless Mode: AP support wireless mode. It may support 802.11a, 802.11b, 802.11g or 802.11n wireless mode.
- Security-Enable: Indicates if the AP provides a security-enabled wireless network.
- Signal: Receive signal strength of the specified network.

Icons and buttons:

: Indicates that the connection is successful.

: Indicates the network type is in infrastructure mode.

: Indicates the network type is in Ad-hoc mode.

: Indicates that the wireless network is security-enabled.

: Indicates 802.11a wireless mode.

: Indicates 802.11b wireless mode.

: Indicates 802.11g wireless mode.

: Indicates 802.11n wireless mode.

: Indicate that the AP list is sorted by SSID, Channel or Signal.

: Button to connect to the selected network.

: Issues a rescan command to the wireless NIC to update information on the surrounding wireless network.

: Adds the selected AP to the Profile setting. It will bring up a profile page and save the user's setting to a new profile.

Connected network:

- When RaUI first runs, it will select the best AP to connect to automatically.
- If the user wants to use another AP, they can click "Connect" for the intended AP to make a connection.
- If the intended network uses encryption other than "Not Use," RaUI will bring up the security page and let the user input the appropriate information to make the connection. Please refer to the example on how to fill in the security information.

When you double click an AP, you can see detailed information about that AP.

The detailed AP information is divided into three parts. They are General, WPS, CCX information and 802.11n (The 802.11n button only exists for APs supporting N mode.) The introduction is as follows:

- General information contains the AP's SSID, MAC address, authentication type, encryption type, channel, network type, beacon interval, signal strength and supported rates. It is shown in Figure 2-3-1-2.

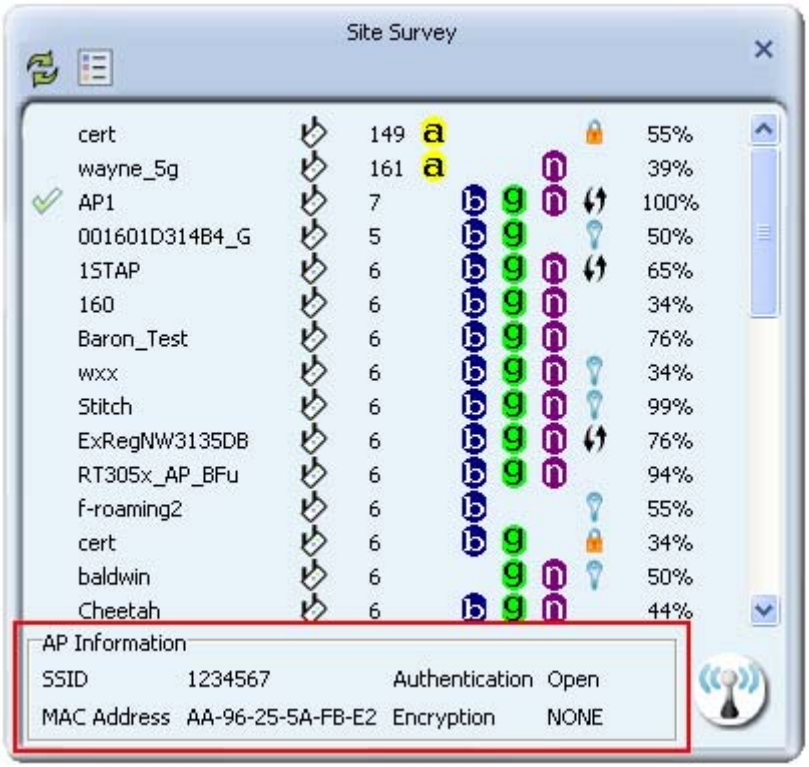
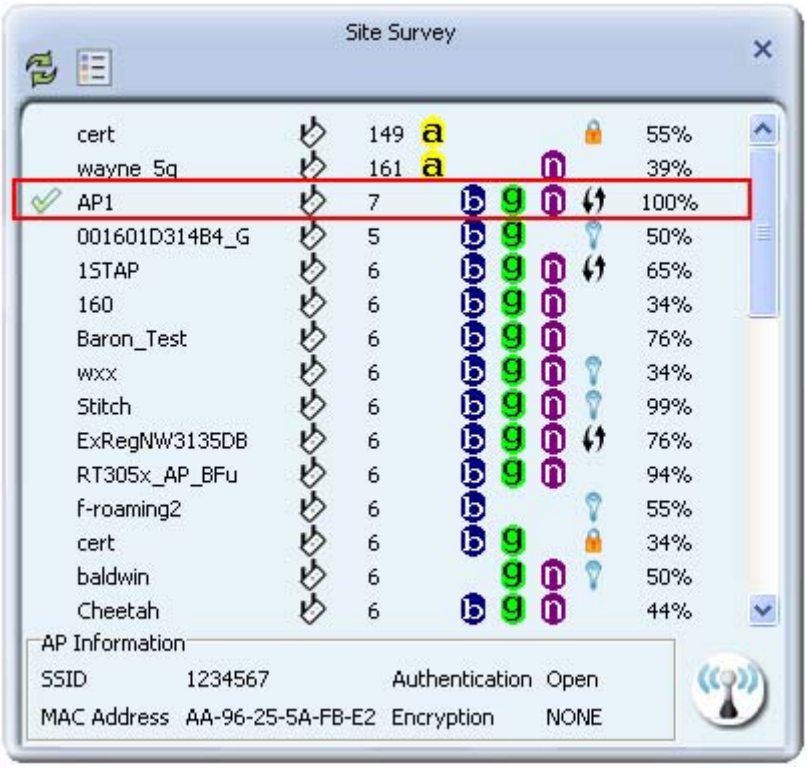


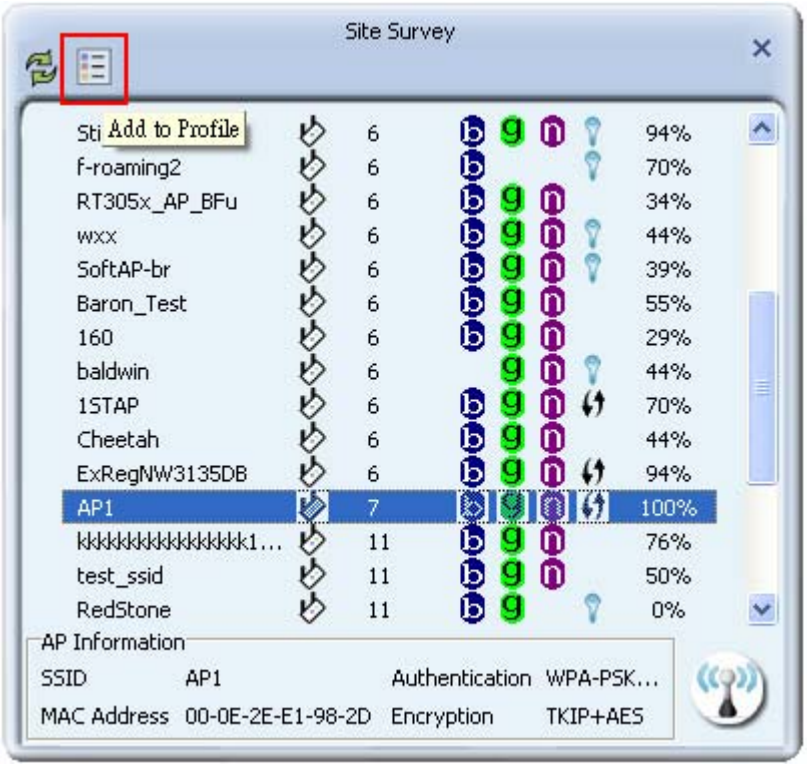
Figure 2-3-1-2 General information about the Access Point

2.3.2 Example on Adding Profile in Network

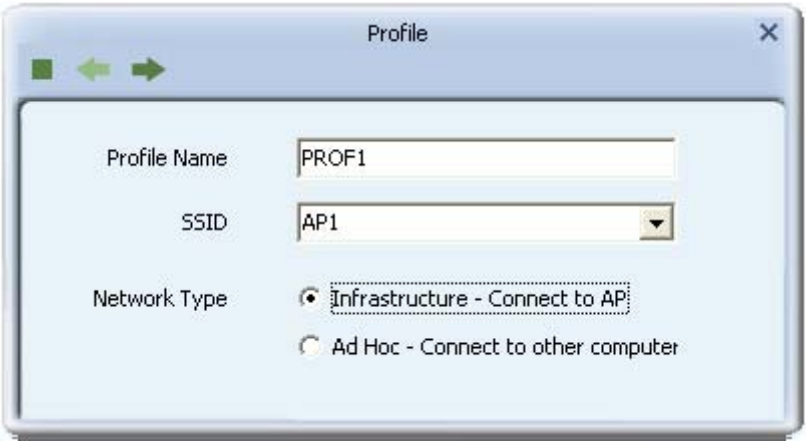
- Select the AP from the list on the Network tab



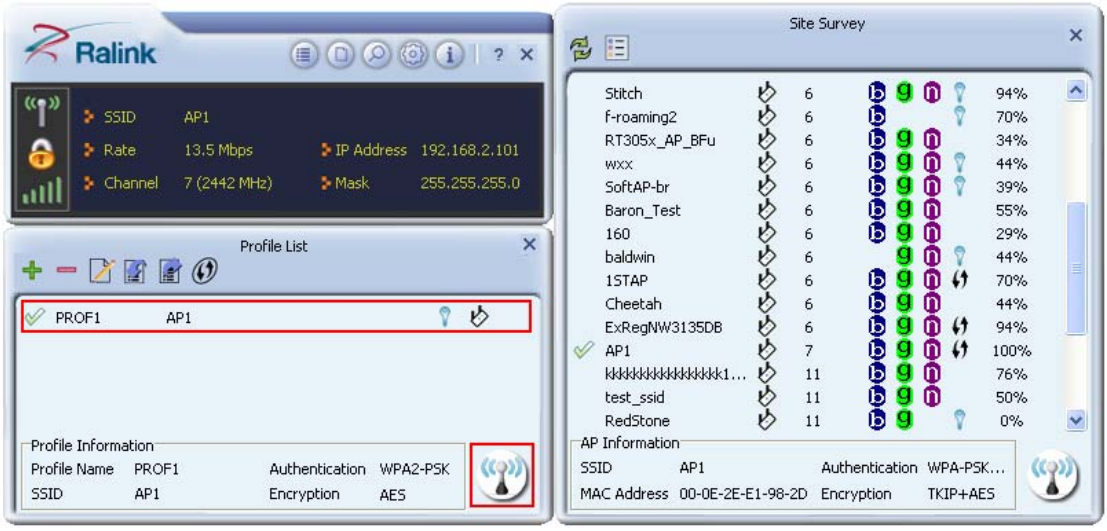
- Click "Add to Profile"



- The System section will appear at the bottom of the Add Profile window. You can specify your own profile name.



- Next, you will see the new profile in the profile list. Click "Activate"



2.4 Advanced

2.4.1 Advanced

Figure 2-4 shows the Advance functions of RaUI.

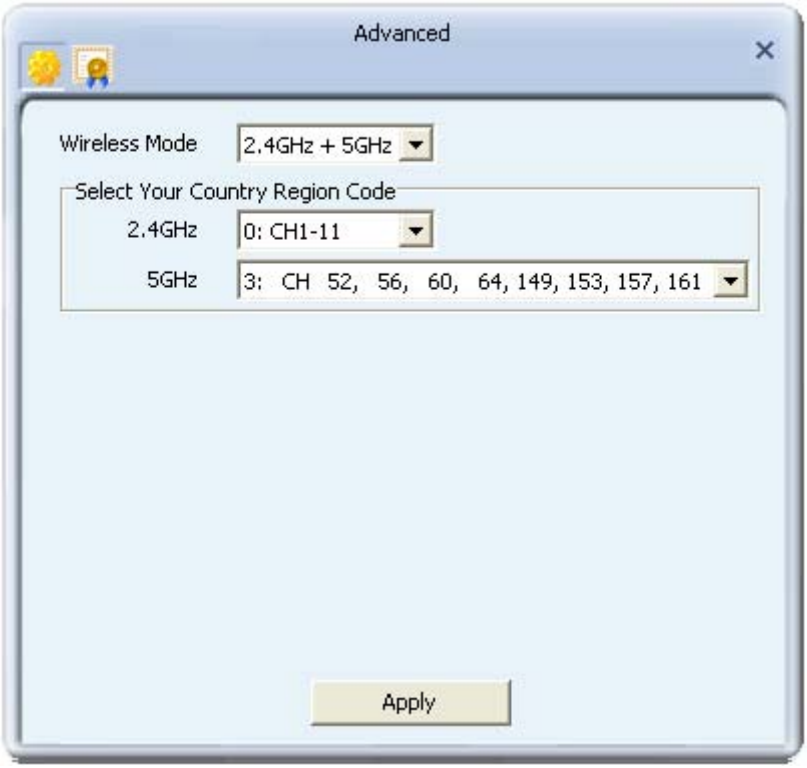


Figure 2-4 Advance function

- Wireless mode: Select wireless mode. 2.4G, 5G and 2.4+5G are supported.(2.4G/5GHz options are depend on different products)
- Wireless Protection: Users can choose from Auto, on, and off. (This is not supported by 802.11n adapters.)

Auto: STA will dynamically change as AP announcement.

On: The frames are always sent with protection.

Off: The frames are always sent without protection.

- TX Rate: Manually select the transfer rate. The default setting is auto. (802.11n wireless cards do not allow the user to select the TX Rate.)
- Enable TX Burst: Ralink's proprietary frame burst mode.
- Enable TCP Window Size: Optimize the TCP window size to allow for greater throughput.
- Fast Roaming at-: enables fast roaming, which is set by the transmit power.
- Select Your Country Region Code: There are eight countries to choose from in the country channel list. (11A ListBox only shows for 5G adapters.)
- Show Authentication Status Dialog: When you connect to an AP with authentication, choose whether show the "Authentication Status Dialog" or not. The Authentication Status Dialog displays the processes during 802.1x authentication.
- Apply the above changes.

2.4.2 Certificate Management

The Certificate Management configuration page as shown in Figure 2-4-2.

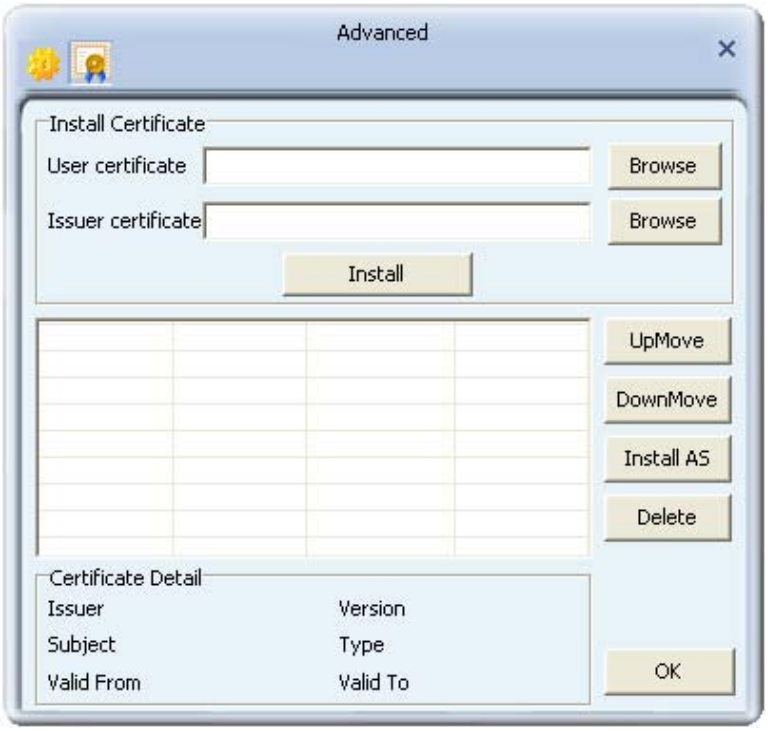


Figure 2-4-2 Certificate Management function

2.5 Link Information

2.5.1 Link Status

The link status page displays detailed information about the current connection as shown in Figure 2-5-1.

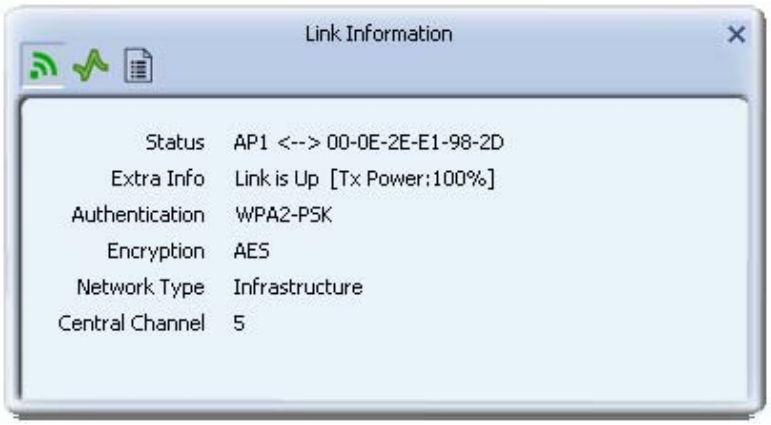


Figure 2-5-1 Link Status function

- Status: Current connection status. If no connection, if will show Disconnected. Otherwise, the SSID and BSSID will show here.
- Extra Info: Display link status in use.
- Channel: Display current channel in use.
- Authentication: Authentication mode in use.
- Encryption: Encryption type in use.
- Network Type: Network type in use.
- IP Address: IP address about current connection.

2.5.2 Throughput

The throughput page displays detailed information about the current connection as shown in Figure 2-5-2.

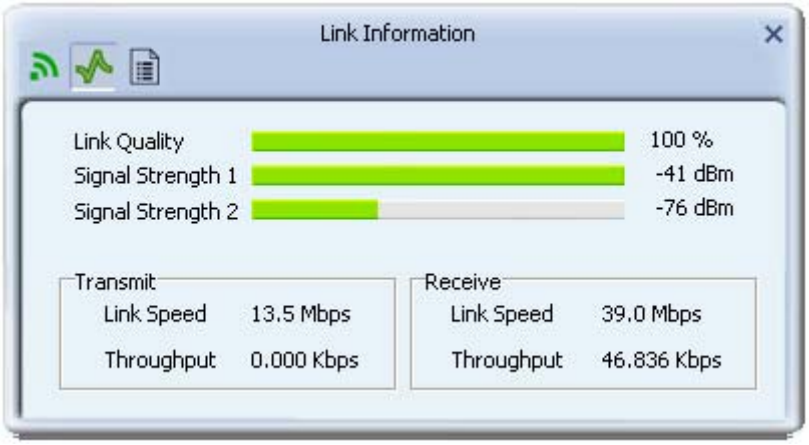


Figure 2-5-2 Throughput function

- Link Speed: Show current transmit rate and receive rate.
- Throughout: Display transmits and receive throughput in unit of Mbps.
- Link Quality: Display connection quality based on signal strength and TX/RX packet error rate.
- Signal Strength 1: Receive signal strength 1, user can choose to display as percentage or dBm format.
- Signal Strength 2: Receive signal strength 2, user can choose to display as percentage or dBm format.
- Signal Strength 3: Receive signal strength 3, user can choose to display as percentage or dBm format.

2.5.3 Statistics

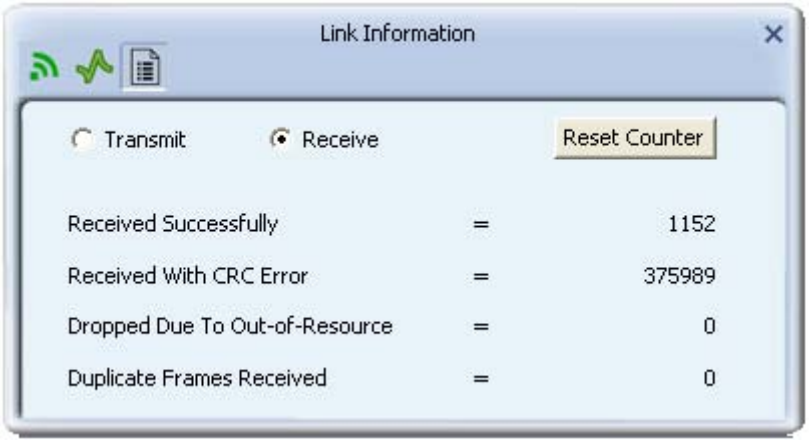
The Statistics page displays detailed counter information based on 802.11 MIB counters. This page translates that MIB counters into a format easier for the user to understand. Figure 2-5-1 shows the detailed page layout.

Figure 2-5-1 Statistics function

Transmit Statistics:

- Frames Transmitted Successfully: Frames successfully sent.
- Frames Fail To Receive ACK After All Retries: Frames failed transmit after hitting retry limit.
- RTS Frames Successfully Receive CTS: Successfully receive CTS after sending RTS frame.
- RTS Frames Fail To Receive CTS: Failed to receive CTS after sending RTS.
- Frames Retransmitted Successfully: Successfully retransmitted frames numbers.
- Reset counters to zero.

Receive Statistics:



- Frames Received Successfully: The number of frames successfully received.
- Frames Received With CRC Error: The number of frames received with a CRC error.
- Frames Dropped Due to Out-of-Resource: The number of frames dropped due to a resource issue.
- Duplicate Frames Received: The number of duplicate frames received.
- Reset all the counters to zero.

2.6 About

2.6.1 About

Click "About" displays the wireless card and driver version information as shown in Figure 2-10.

Figure 2-10 About function

Connect to Ralink's website: Ralink Technology, Corp.

Display Configuration Utility, Driver, and EEPROM version information.

Display Wireless NIC MAC address.

2.7 WPS

2.7.1 WPS

Figure 2-7-1 illustrates the RaUI WPS functions.

Figure 2-7-1 WPS function

- WPS Configuration: The primary goal of Wi-Fi Protected Setup (Wi-Fi Simple Configuration) is to simplify the security setup and management of Wi-Fi networks. Ralink STA supports the configuration and setup using a PIN configuration method or a PBC configuration method through an internal or external Registrar.
- WPS AP List: Displays the SSID of the surrounding APs with WPS IE from the last scan result.
- PBC: Start to add to AP using PBC configuration method.
- PIN: Start to add to Registrar using PIN configuration method. If STA Registrar, remember that enter PIN Code read from your Enrollee before starting PIN.
- Auto: Starts to add to AP by using to select the AP automatically in PIN method.

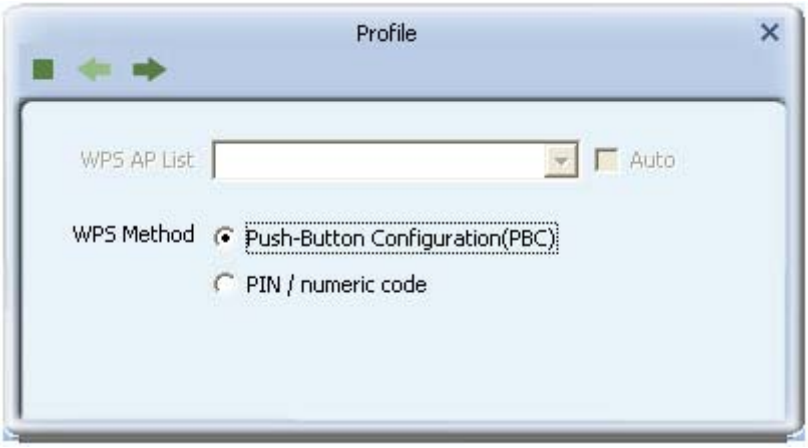


Figure 2-7-1-1 WPS Profile

- PIN Code: The user is required to enter an 8-digit PIN Code into Registrar. When an STA is the Enrollee, you can click "Renew" to re-generate a new PIN Code.
- Config Mode: The station serving as an Enrollee or an external Registrar.

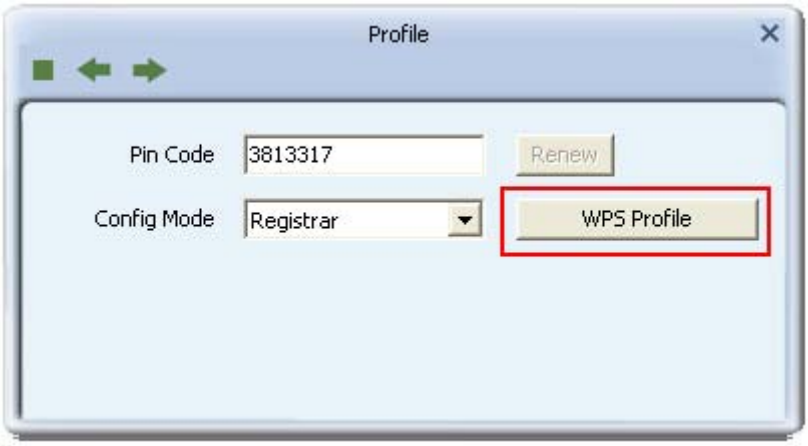


Figure 2-7-1-2 WPS PIN function

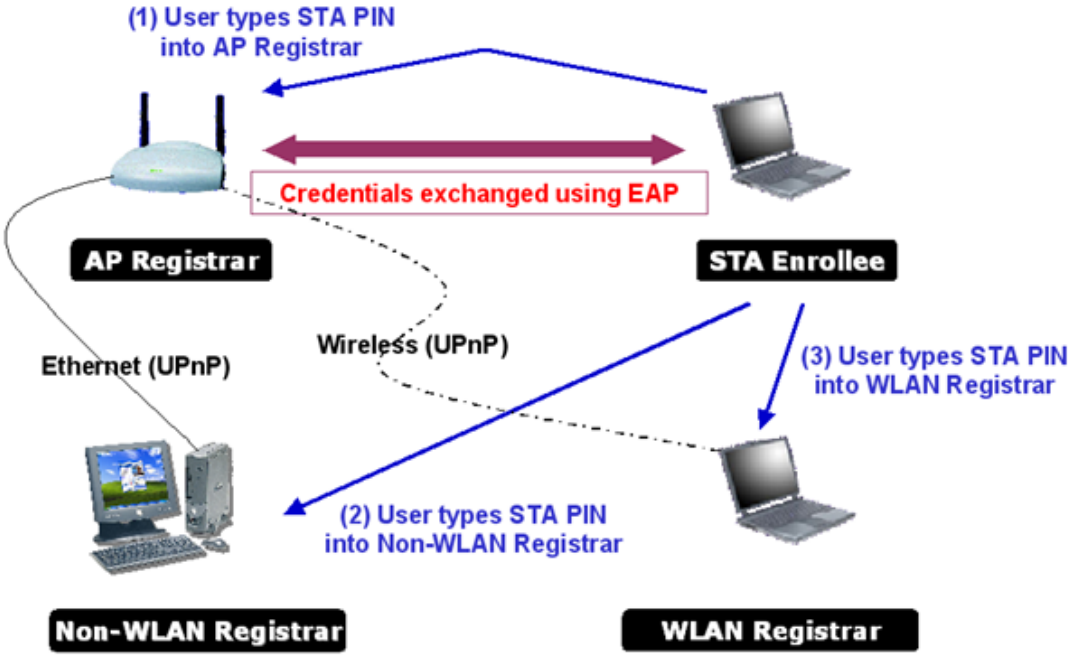
After the user clicks PIN or PBC, please do not rescan within two-minutes of the connection. If you want to abort this setup within the interval, restart PIN/PBC or click "Disconnect" to stop WPS action.

- Progress Bar: Displays the rate of progress from Start to Connected.
- Status Bar: Displays the current WPS Status.

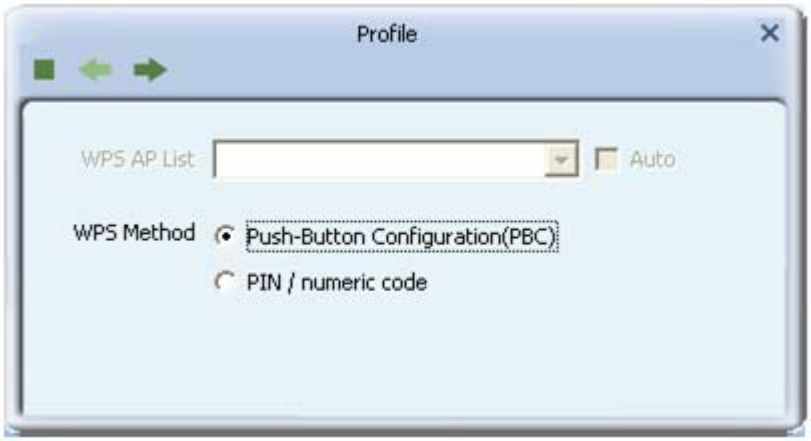
There are examples in section 2-7-3(PIN Enrollee Setup), section 2-7-4(PBC Enrollee Setup) and section 2-7-5(Registrar Configures and AP)

2.7.2 Example to Add to Registrar Using PIN Method

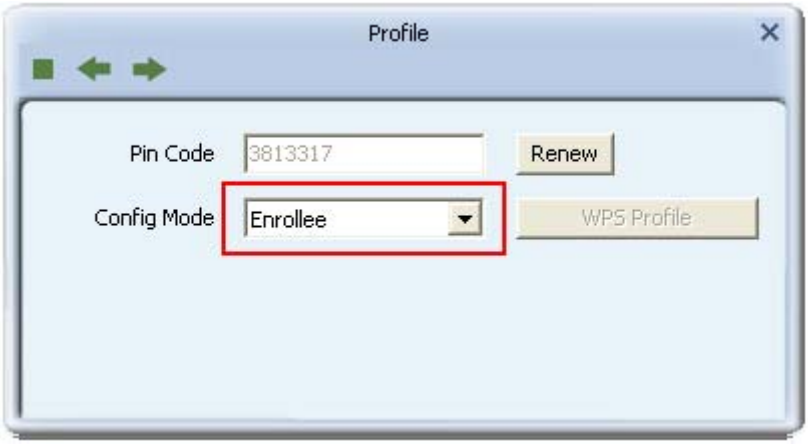
The user obtains a device password (PIN Code) from the STA and enters the password into the Registrar. Both the Enrollee and the Registrar use PIN Config method for the configuration setup. The following image outlines the process.


(1) User types STA PIN into AP Registrar
Credentials exchanged using EAP
AP Registrar
STA Enrollee
Wireless (UPnP)
Ethernet (UPnP)
(3) User types STA PIN into WLAN Registrar
(2) User types STA PIN into Non-WLAN Registrar
Non-WLAN Registrar
WLAN Registrar

- Select an AP (SSID/BSSID) that STA will join to and Select the “PIN/numeric code” method.



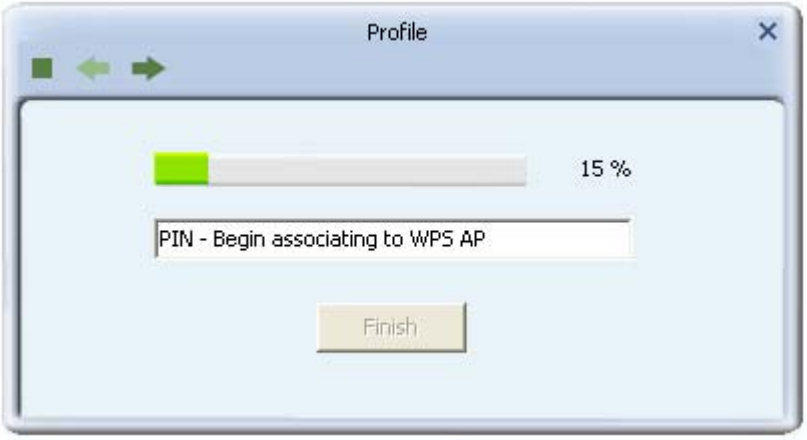
- Select "Enrollee" from the Config Mode drop-down list.
- Enter the PIN Code of the STA into the Registrar when prompted by the Registrar.



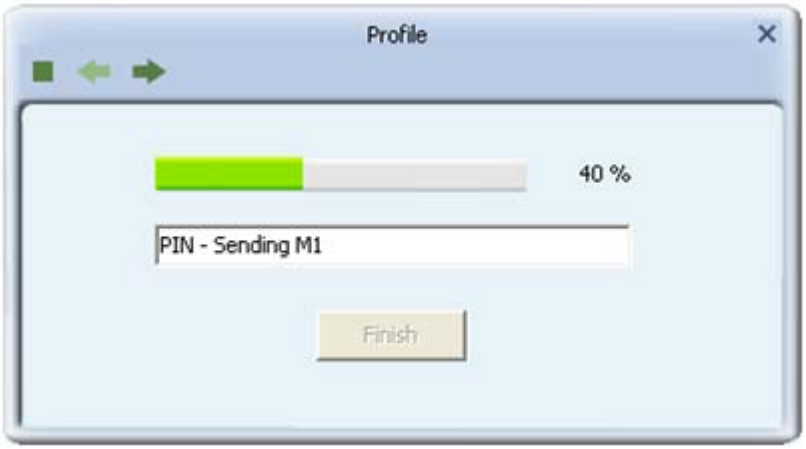
If you use Microsoft Window Connection Now as an External Registrar, you must start PIN connection at STA first. After that, search out your WPS Device name and MAC address at Microsoft Registrar. Add a new device and enter PIN Code of STA at Microsoft Registrar when prompted.

- Click “PIN” to enter the PIN

- The result should appear as the image below.



- Configure one or more credentials



- Then connect successfully. The result appears as the following image.

- Click “Finish”

Describe "WPS Status Bar" - "PIN - xxx" as follow:

- Acceptable PIN Configurations:

Start PIN connection - SSID ~> Begin associating to WPS AP ~> Associated to WPS AP ~> Sending EAPOL-Start ~> Sending EAP-Rsp (ID) ~> Receive EAP-Req (Start) ~> Sending M1 ~> Received M2 ~> (Received M2D ~> Sending EAP-Rsp (ACK)) ~> Sending M3 ~> Received M4 ~> Sending M5 ~> Received M6 ~> Sending M7 ~> Received M8 ~> Sending EAP-Rsp(Done) ~> Configured ~> WPS status is disconnected ~> WPS status is connected successfully-SSID

- WPS configuration doesn't complete after a two-minute connection:

WPS EAP process failed.

- When errors occur within **two minutes of connecting**, the WPS status bar might report "WPS EAP process failed".

Error messages might be:

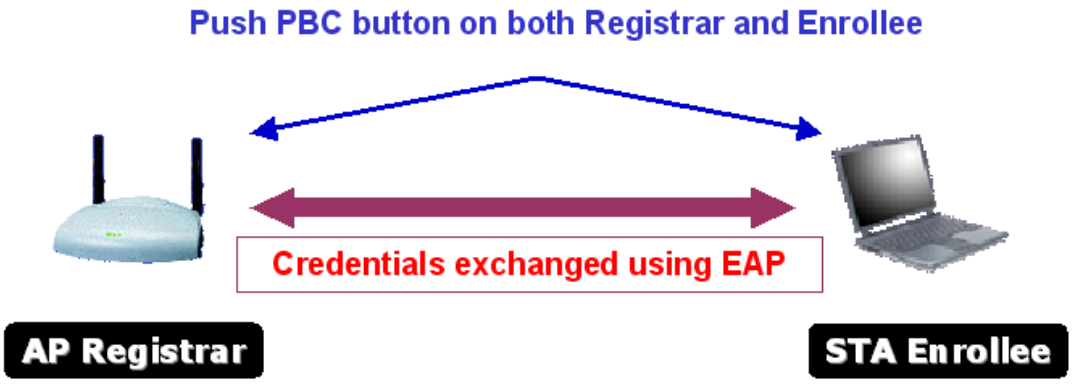
1. Receive EAP with wrong NONCE.
2. Receive EAP without integrity.
3. Error PIN Code.
4. An inappropriate EAP-FAIL received.

2.7.3 Example to Add to Registrar Using PBC Method

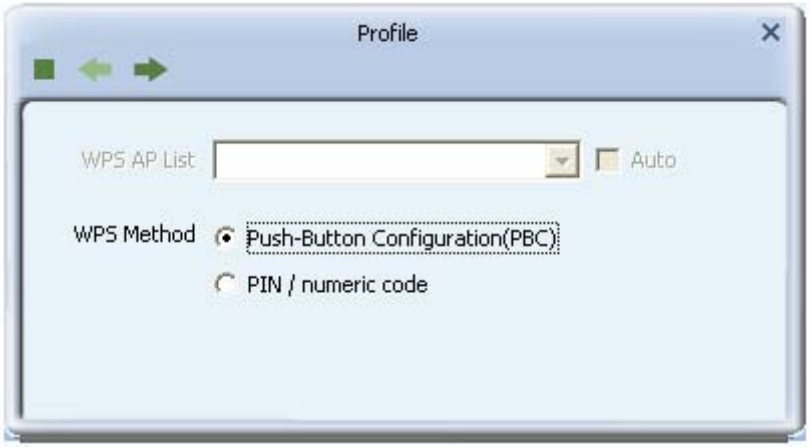
The PBC method requires the user to press a PBC button on both the Enrollee and the Registrar within a two-minute interval called the Walk Time. If there is only one Registrar in PBC mode, the PBC mode selected is obtained from ID 0x0004, and is found after a complete scan. The Enrollee can then immediately begin running the Registration Protocol.

If the Enrollee discovers more than one Registrar in PBC mode, it MUST abort its connection attempt at this scan and continue searching until the two-minute timeout.

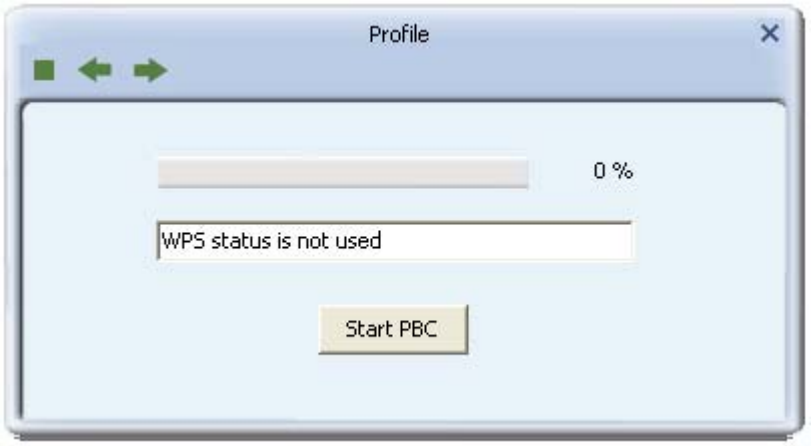
*Before you press PBC on STA and candidate AP. Make sure all APs aren't PBC mode or APs using PBC mode have left their Walk Time.



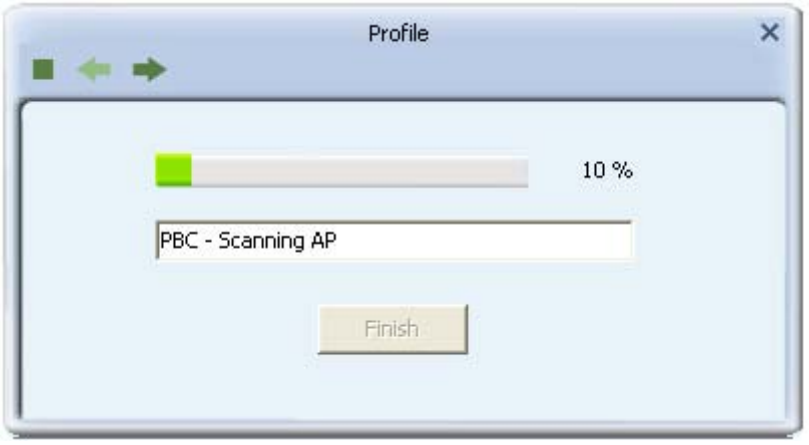
- Select an AP (SSID/BSSID) that STA will join to and Select the “Push-button Configuration” method.



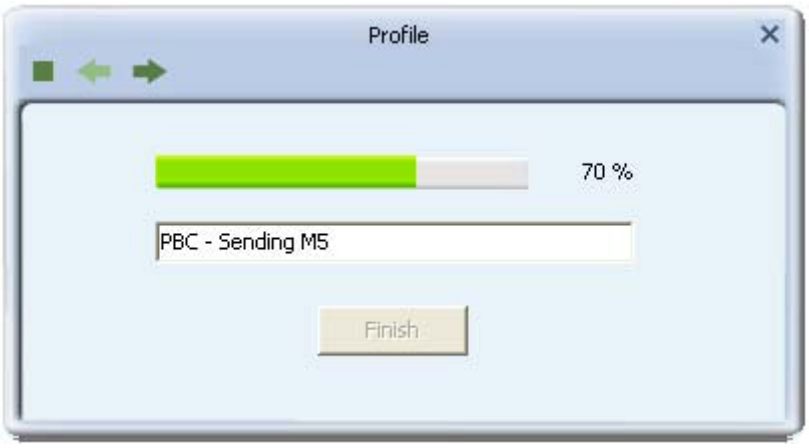
- Click PBC to start the PBC connection.
- Push the PBC on AP.



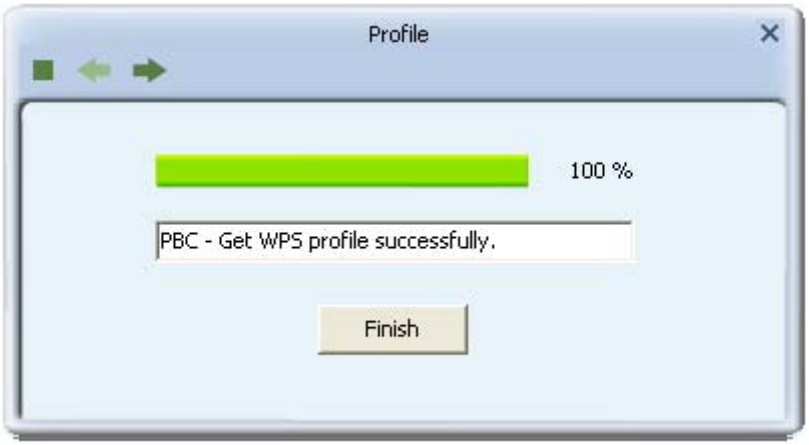
- The progress bar as shown in the figure below indicates that scanning progress.



- When one AP is found, join it.



- Configure and receive one or more credential(s).



- Then connect successfully. The result will be displayed as it is in the figure below.

Describe "WPS Status Bar" - “PBC - xxx" as follow:

- A successful PBC Configuration:

Start PBC connection ~> Scanning AP ~> Begin associating to WPS AP ~> Associated to WPS AP ~> Sending EAPOL-Start ~> Sending EAP-Rsp (ID) ~> Receive EAP-Rsp (Start) ~> Sending M1 ~> Received M2 ~> Sending M3 ~> Received M4 ~> Sending M5 ~> Received M6 ~> Sending M7 ~> Received M8 ~> Sending EAP-Rsp (Done) ~> Configured ~> WPS status is disconnected ~> WPS status is connected successfully-SSID

- No PBC AP available:

Scanning AP ~> No PBC AP available ~> Scanning AP ~> No PBC AP available ~>...

- Too Many PBC AP available:

Scanning AP ~> Too Many PBC AP available ~> Scanning AP ~> Too Many PBC AP available ~>...

- WPS configuration doesn't complete after **two-minute connection**:

WPS EAP process failed.

- When Errors occur within **two-minutes of establishing a connection**, the WPS status bar might report "WPS EAP process failed".

Error messages might be:

1. Receive EAP with wrong NONCE.
2. Receive EAP without integrity.
3. An inappropriate EAP-FAIL received.

Describe "Multiple PBC session overlaps" as follow:

- Dual bands:

AP1 is a G-Band AP using PBC mode. (ID = 0x0004)

AP2 is a A-Band AP using PBC mode. (ID = 0x0004)

They have the same UUID-E.

STA would regard these two APs as a dual-radio AP and select one band to connect.

- Different UUID-E :

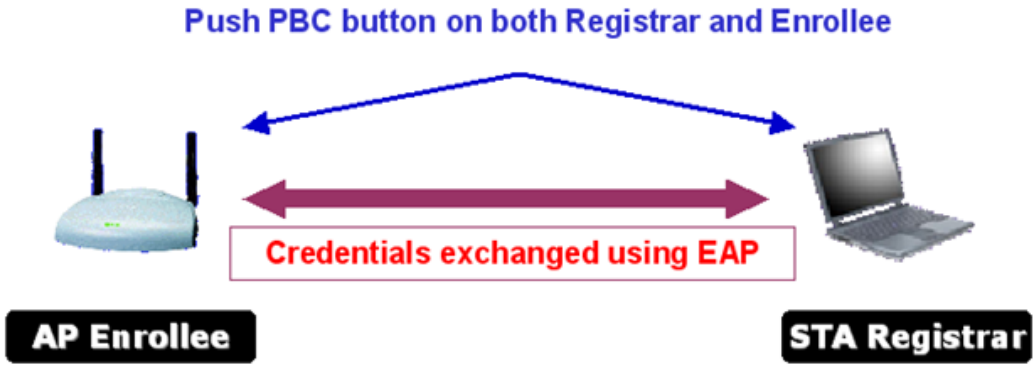
AP1 is a G-Band AP using PBC mode. (ID = 0x0004)

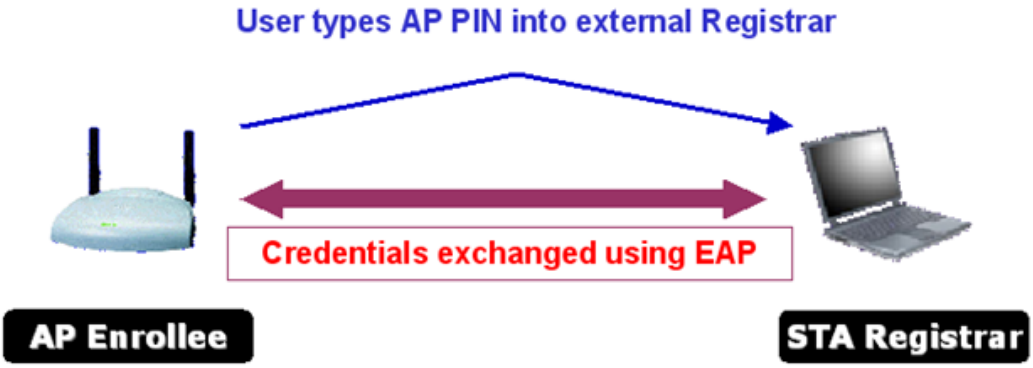
AP2 is a G-Band AP using PBC mode. (ID = 0x0004)

They have the different UUID-E.

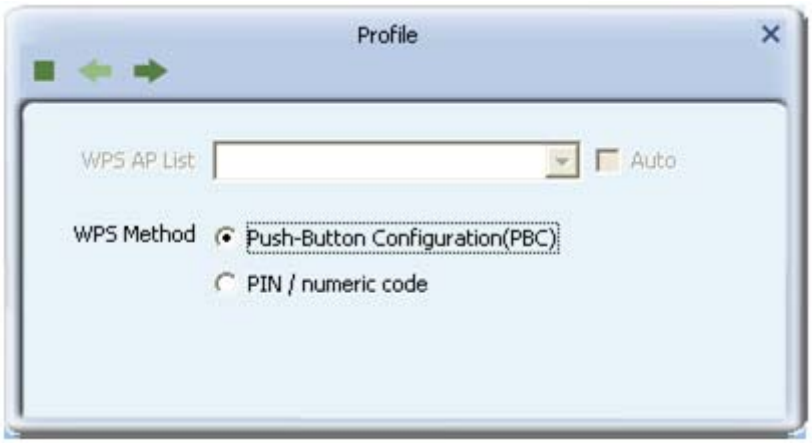
STA would regard these two APs as two different APs and wait until only one PBC AP is available.

2.7.4 Example to Configure a Network/AP Using PIN or PBC Method



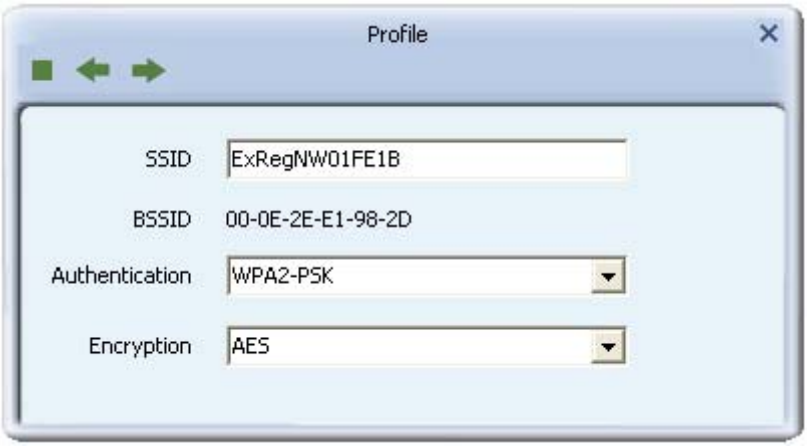


Select an AP (SSID/BSSID) that STA will config and Select the “PIN/numeric code” method.



- Select “Registrar” from the Config Mode drop-down list.
- Enter the PIN Code of the STA into the Registrar when prompted by the Registrar.

- Enter the details of the credential and change configurations (SSID, Authentication, Encryption and Key) manually if needed.



- Start PIN or PBC. The following procedures are as similar as section 2-7-3 (PIN Enrollee Setup) or section 2-7-4(PBC Enrollee Setup),
- If your AP Enrollee has been configured before the WPS process, the credential you set in advance will be updated to the AP itself. Otherwise, after a successful registration, the AP Enrollee will be re-configured with the new parameters, and the STA Registrar will connect to the AP Enrollee with these new parameters.

Describe "WPS Status Bar" - "PIN - xxx" as follow:

A successful PIN Configuration:

Start PIN connection - SSID ~> Begin associating to WPS AP ~> Associated to WPS AP ~> Sending EAPOL-Start ~> Sending EAP-Rsp (ID) ~> Receive M1 ~> Sending M2 ~> Receive M3 ~> Sending M4 ~> Receive M5 ~> Sending M6 ~> Receive M7 ~> Sending M8 ~> Receive EAP Rsp (Done) ~> Sending EAP Rsp (ACK) ~> Configured ~> WPS status is disconnected ~> WPS status is connected successfully-SSID

Describe "WPS Status Bar" - “PBC - xxx" as follow:

A successful PBC Configuration:

Start PBC connection ~> Scanning AP ~> Begin associating to WPS AP ~> Associated to WPS AP ~> Sending EAPOL-Start ~> Sending EAP-Rsp (ID) ~> Receive M1 ~> Sending M2 ~> Receive M3 ~> Sending M4 ~> Receive M5 ~> Sending M6 ~> Receive M7 ~> Sending M8 ~> Receive EAP Rsp (Done) ~> Sending EAP Rsp (ACK) ~> Configured ~> WPS status is disconnected ~> WPS status is connected successfully-SSID

3. Security

3.1 Auth.\ Encry. Setting – WEP/TKIP/AES

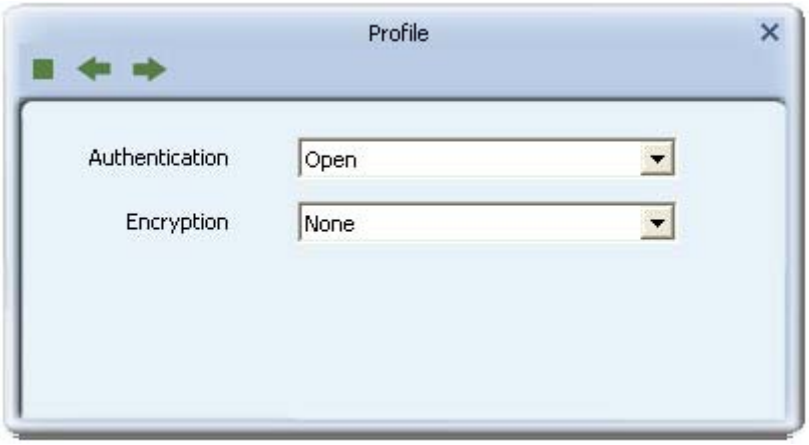


Figure 3-1 Auth.\Encry. Settings in the Profile Page

- Authentication Type: There are 7 authentication modes supported by RaUI. They are Open, Shared, WPA and WPA-PSK, WPA2 and WPA2-PSK, 802.1x, WAPI-PSK and WAPI-CA.
- Encryption Type: For open and shared authentication mode, the available encryption types are none and WEP. For Shared and 802.1x authentication mode, the selection of available encryption is WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode, both TKIP and AES encryption is available. For WAPI-PSK and WAPI-CA authentication mode, only SMS4 encryption is available.

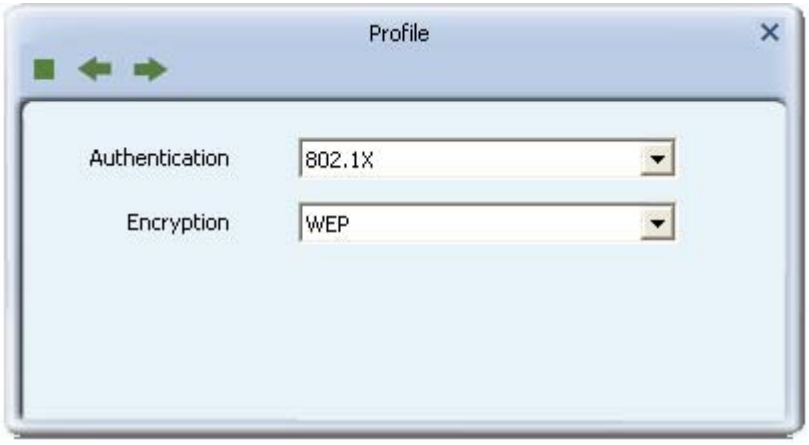


Figure 3-1-2 Authentication \ Encryption Settings in the Profile Page

- 8021X: This is introduced in the topic of Section 3-2.

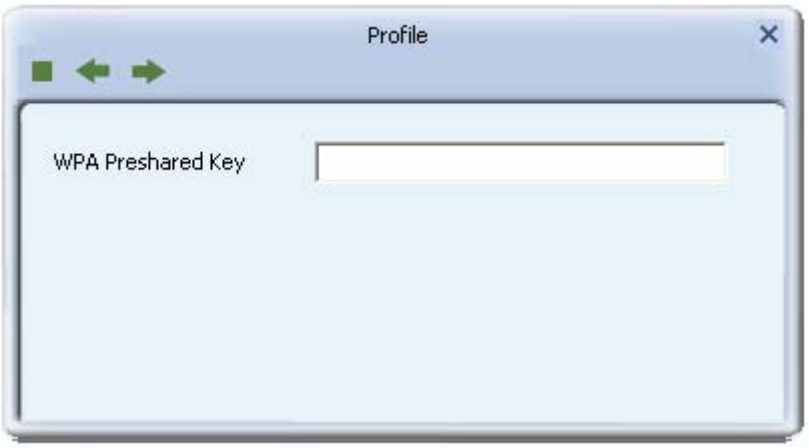


Figure 3-1-3 Pre-shared Key Configuration

- Pre-shared Key: This is the shared key between the AP and STA. If operating in WPA-PSK and WPA2-PSK authentication mode, this field must be filled with a key between 8 and 32 characters in length.

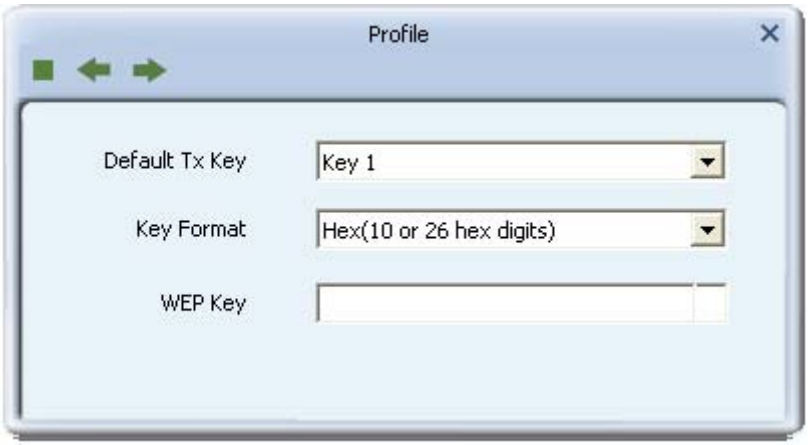
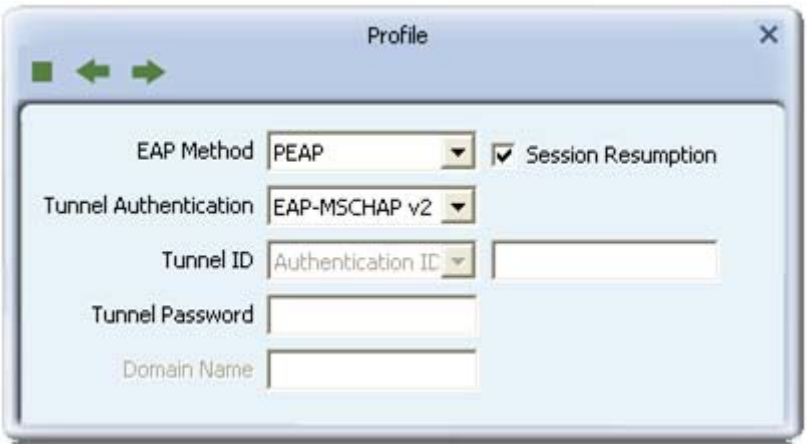


Figure 3-1-4 WEP Key Configuration

- WEP Key: Only valid when using WEP encryption algorithm. The key must match the AP's key. There are several formats to enter the keys.
    1. Hexadecimal - 40bits: 10 Hex characters.
    2. Hexadecimal - 128bits: 32Hex characters.
    3. ASCII - 40bits: 5 ASCII characters.
    4. ASCII - 128bits: 13 ASCII characters.

3.2 802.1x Setting

802.1x is used for authentication of the "WPA" and "WPA2" certificate by the server.



Authentication type:

- PEAP: Protect Extensible Authentication Protocol. PEAP transport securely authenticates data by using tunneling between PEAP clients and an authentication server. PEAP can authenticate wireless LAN clients using only server-side certificates, thus simplifying the implementation and administration of a secure wireless LAN.
- TLS/Smart Card: Transport Layer Security. Provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys to secure subsequent communications between the WLAN client and the access point.
- TTLS: Tunneled Transport Layer Security. This security method provides for certificate-based, mutual authentication of the client and network through an encrypted channel. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.
- EAP-FAST: Flexible Authentication via Secure Tunneling. It was developed by Cisco. Instead of using a certificate, mutual authentication is achieved by means of a PAC (Protected Access Credential) which can be managed dynamically by the authentication server. The PAC can be supplied (distributed one time) to the client either manually or automatically. Manually, it is delivered to the client via disk or a secured network distribution method. Automatically, it is supplied as an in-band, over the air, distribution. For tunnel authentication, only support "Generic Token Card" authentication.
- LEAP: Light Extensible Authentication Protocol is an EAP authentication type used primarily by Cisco Aironet WLANs. It encrypts data transmissions using dynamically generated WEP keys, and supports mutual authentication.
- MD5-Challenge: Message Digest Challenge. Challenge is an EAP authentication type that provides base-level EAP support. It provides for only one-way authentication - there is no mutual authentication of wireless client and the network.(Only support XP)

Session Resumption: The user can choose "Disable" and "Enable".

Tunnel Authentication:

- Protocol: Tunnel protocol, List information include "EAP-MSCHAP v2", "EAP-TLS/Smart card", "Generic Token Card", "CHAP", "MS-CHAP", "MS-CHAP-V2", "PAP" and "EAP-MD5".
- Tunnel Identity: Identity for tunnel.

- Tunnel Password: Password for tunnel.

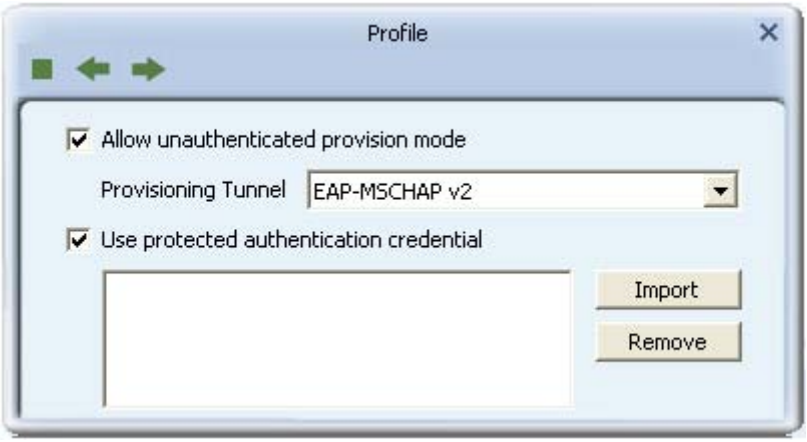
ID \ PASSWORD

- Authentication ID/Password: The identity, password and domain name for server. Only "EAP-FAST" and "LEAP" authentication can key in domain name. Domain names can be keyed in the blank space.
- Tunnel ID/Password: Identity and Password for the server..

Client Certification

Use Client certificate: Client certificate for server authentication.

EAP Fast



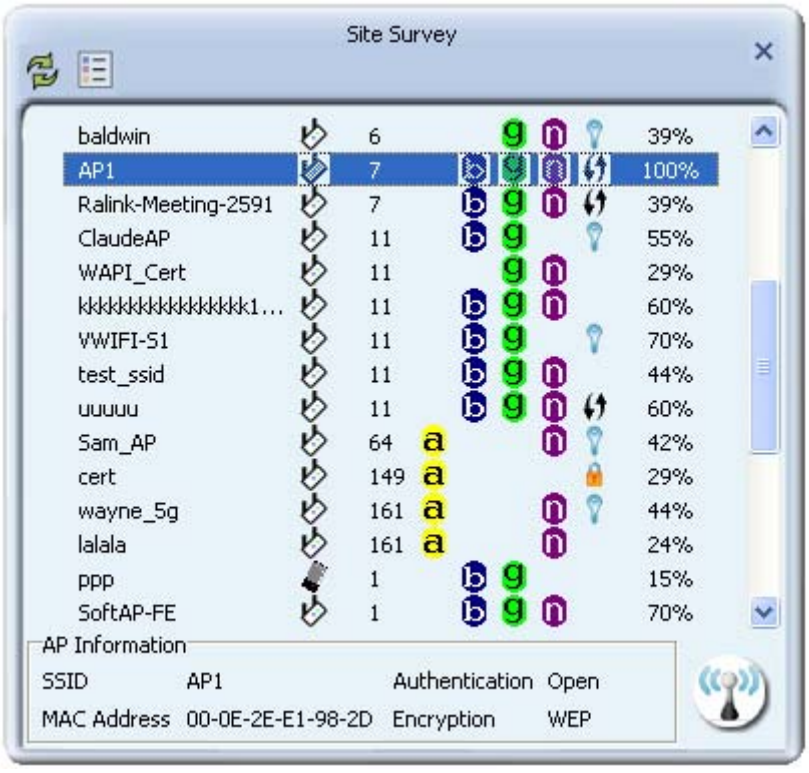
- Allow unauthenticated provision mode: During the PAC can be provisioned (distributed one time) to the client automatically. It only supported "Allow unauthenticated provision mode" and use "EAP-MSCHAP v2" authentication to authenticate now. It causes to continue with the establishment of the inner tunnel even though it is made with an unknown server.
- Use protected authentication credential: Using PAC, the certificate can be provided to the client manually via disk or a secured network distribution method.

Server Certification

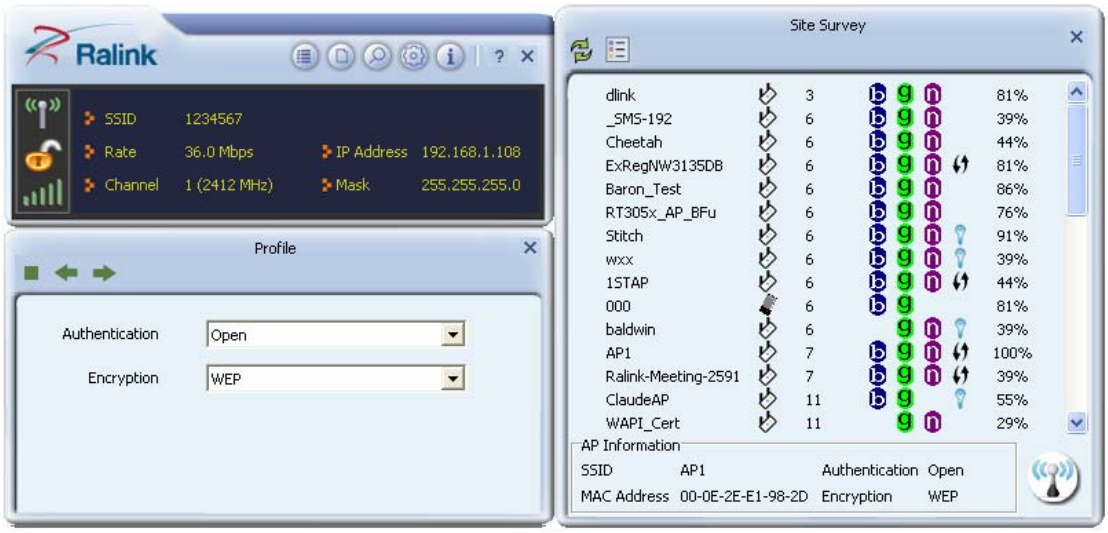
- Certificate issuer: Select the server that issues the certificate.
- Allow intermediate certificates: It must be in the server certificate chain between the server certificate and the server specified in the "certificate issuer must be" field.
- Server name: Enter an authentication sever root.

3.3 Example to Configure Connection with WEP on

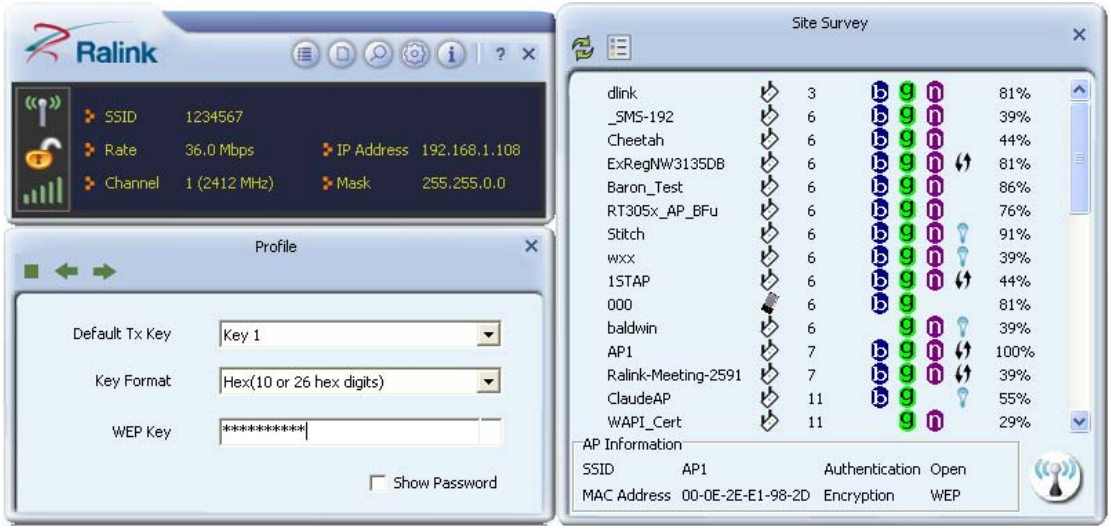
- Select an AP with WEP encryption and click "Connect".



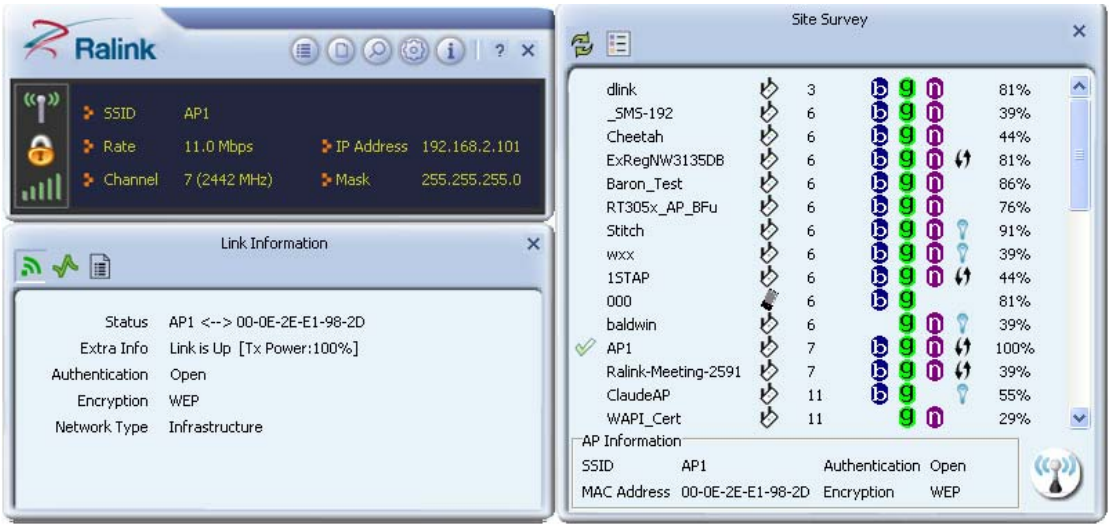
- The Auth.\Encry. function will appear as below;



- Enter 1234567890 in the Key#1 Hexadecimal field. This value is same as our intended AP's setting.

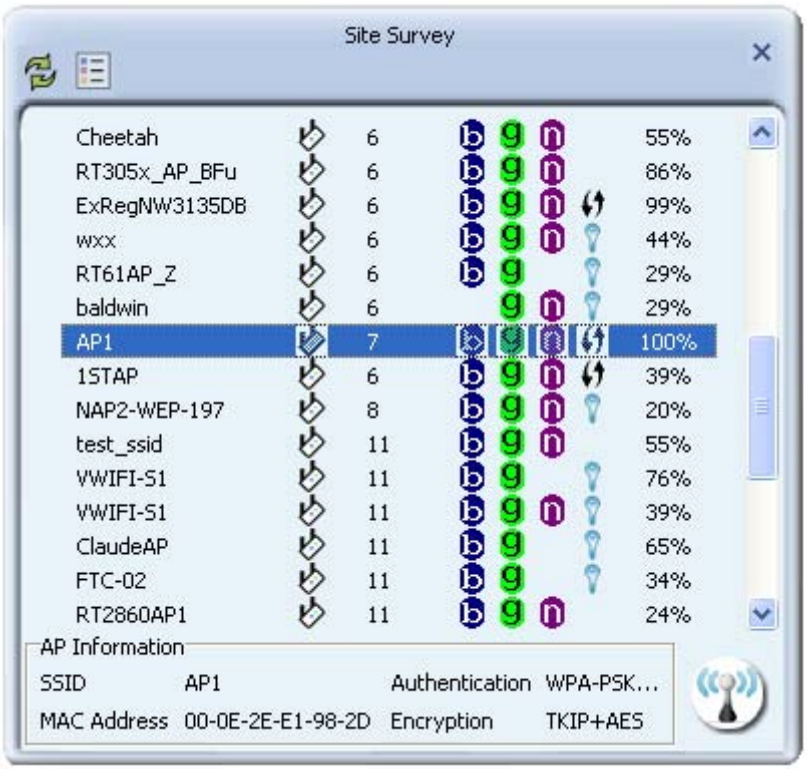


- Click "OK". The dialog box will appear as below;

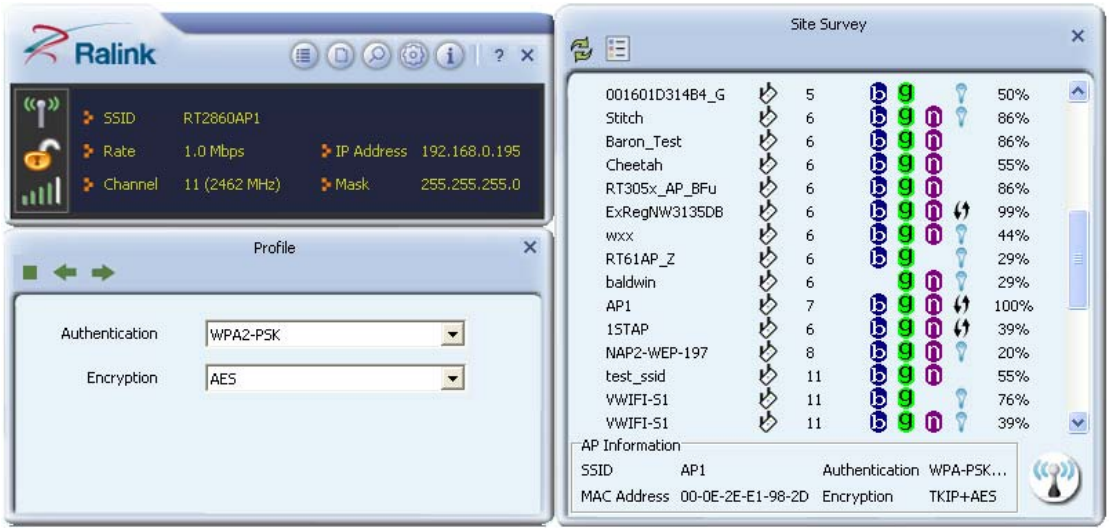


3.4 Example to Configure Connection with WPA-PSK

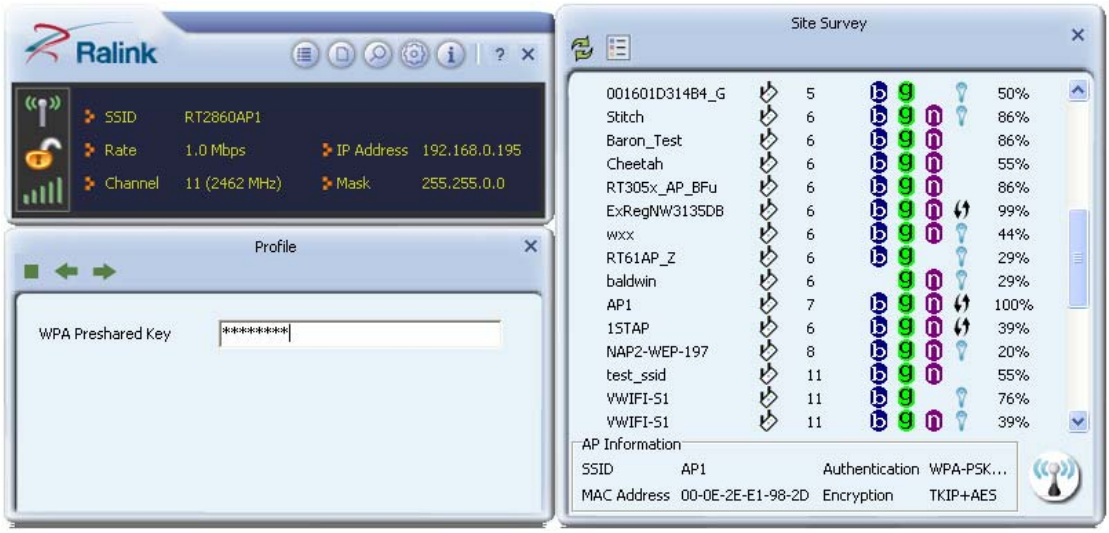
- Select the AP with a WPA-PSK authentication mode and click "Connect".



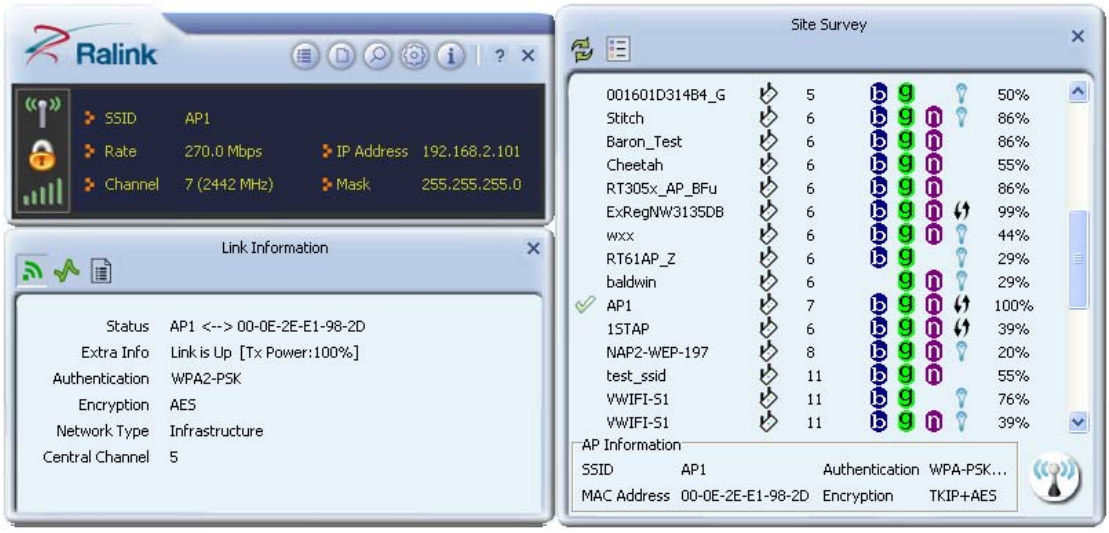
- Auth.\Encry. function appears.



- Select WPA-PSK as the Authentication Type. Select TKIP or AES encryption. Enter the WPA Pre-Shared Key as "12345678".

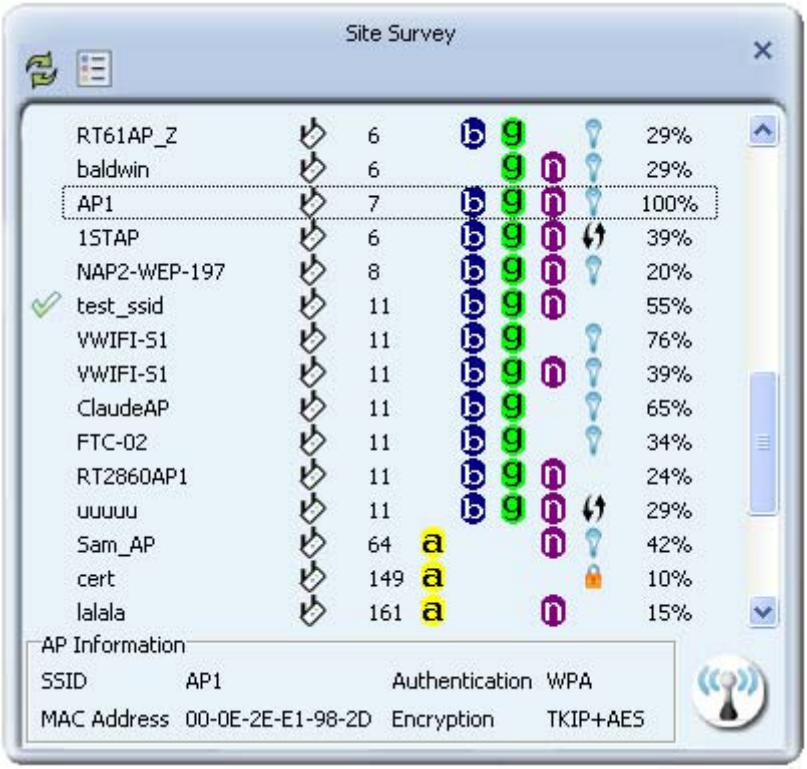


- Click "OK". Be careful, if the WPA Pre-Shared Key entered is not correct, you won’t be able to exchange any data frames, even though the AP can be connected.

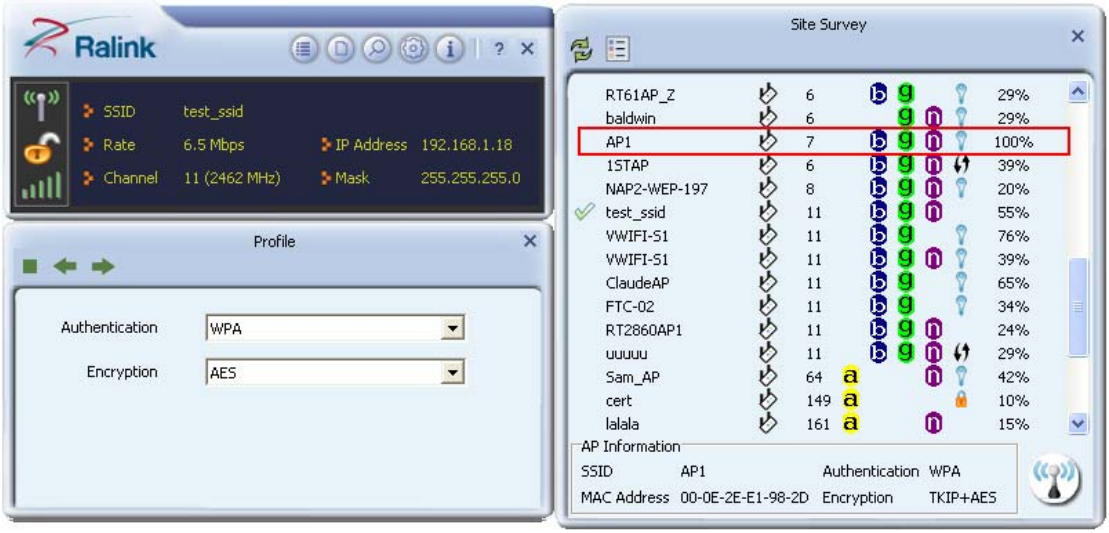


3.5 Example to Configure Connection with WPA

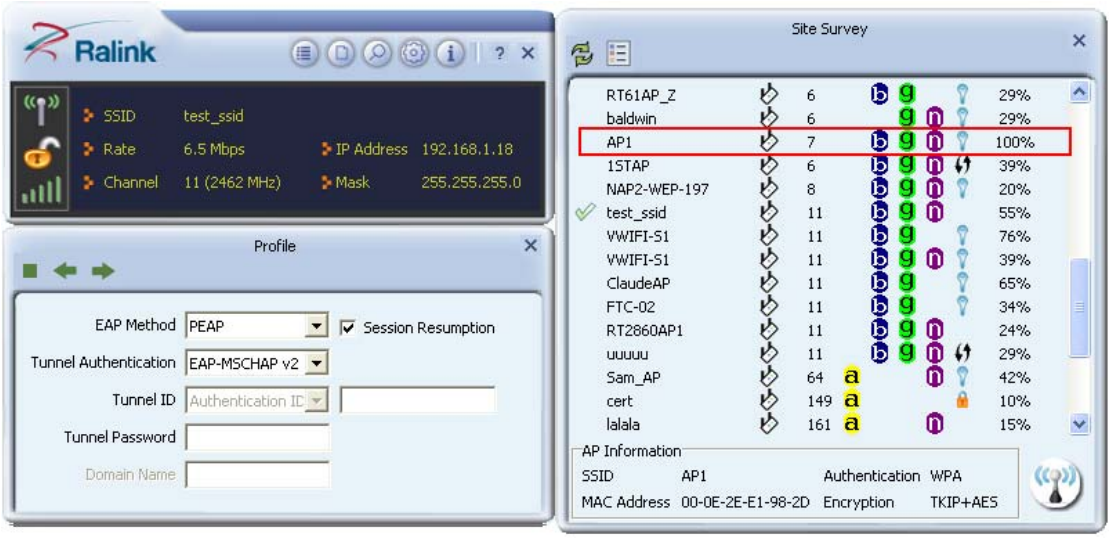
- Select an AP with WPA authentication mode and click "Connect".



- The Auth.\Encry. function pop up. (If AP setup security to Both (TKIP + AES), system defines is AES that security is severely.)



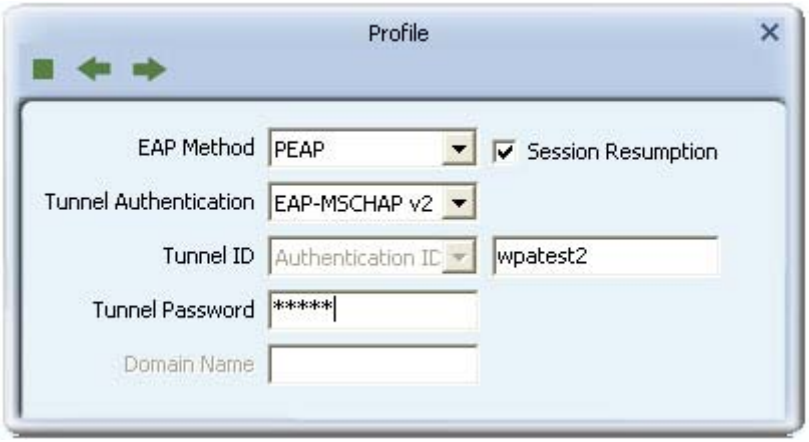
- Click "8021X" and the setting page will appear.



- Authentication type and setting method:

PEAP:

1. Select "PEAP" as the Authentication type from the drop-down list. Key-in "wpatest2" for the identity. "Select "EAP-MSCHAP v2" from the drop-down list for tunnel authentication and key-in the tunnel identity as "wpatest2" and the tunnel password as "test2". These settings are the same as our intended AP's setting.

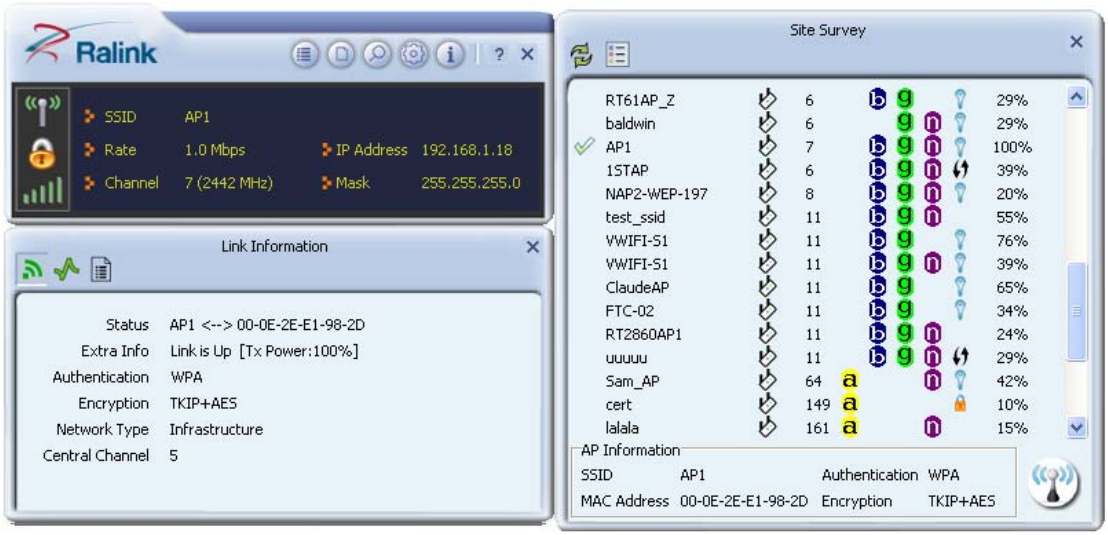


2. Click to next page.

*If you want to disconnect, please click cancel button in Authentication Status function.

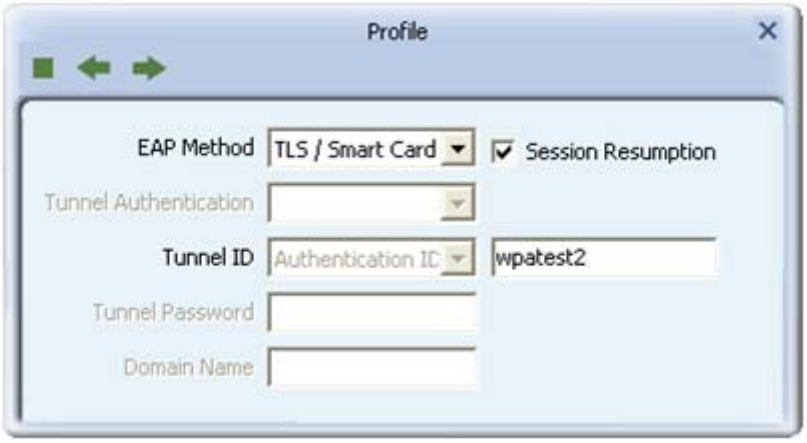
*In Profile function, show "Profile Name" option only in adding AP to Profile function.

3. If the connection is successful, the dialog will appear as below.



TLS / Smart Card:

1. "Select TLS / Smart Card" from the Authentication type drop-down list. TLS only requires the identification to be set as "wpatest2" for server authentication.



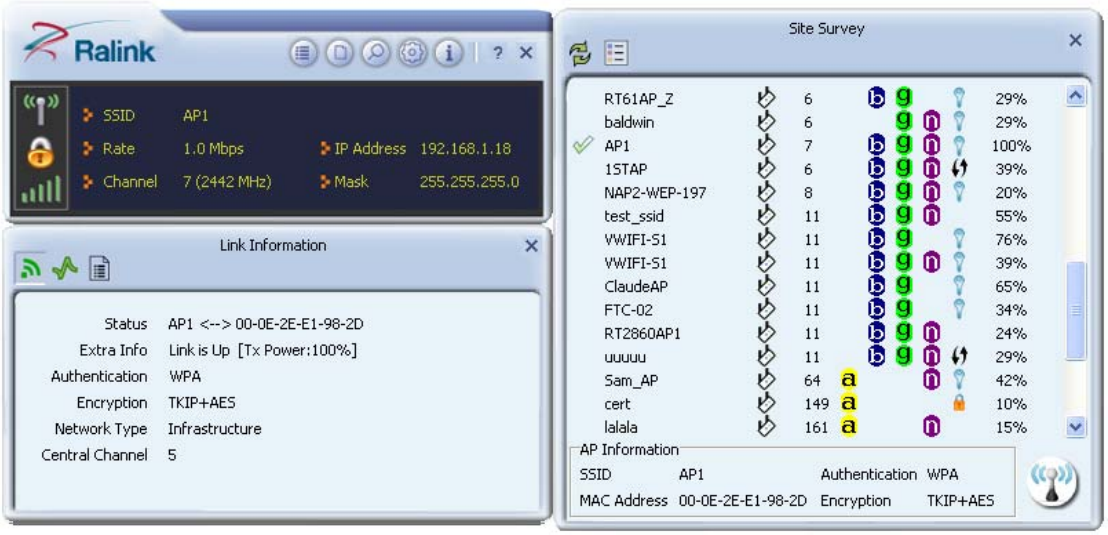
2. TLS must use client certification. Click "Client Certification" and select a certification for server authentication.

3. Click to the next page.

*If you want to disconnect, please click "Cancel" on the Authentication Status function page.

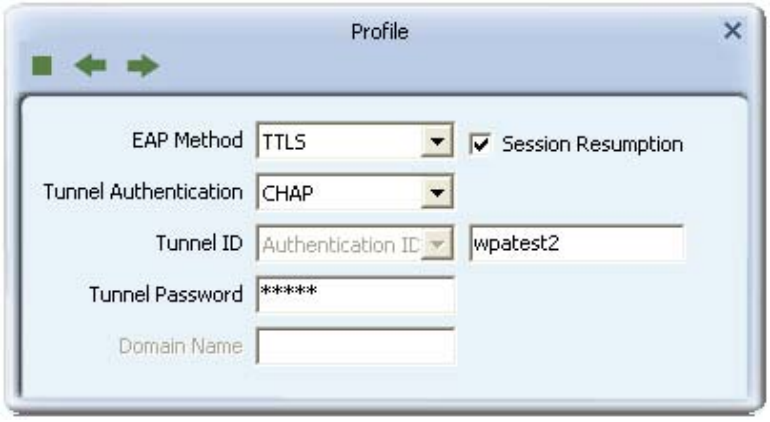
*In Profile function, show "Profile Name" option only in adding AP to Profile function.

4. If it connected successfully, the result will appear as in the image below.



TTLS:

1. Select TTLS from the Authentication type drop-down list. Key-in the identity as "wpatest2". Select CHAP for tunnel authentication, and key-in the identity as "wpatest2" and tunnel password as "test2". These settings are the same as our intended AP's setting.

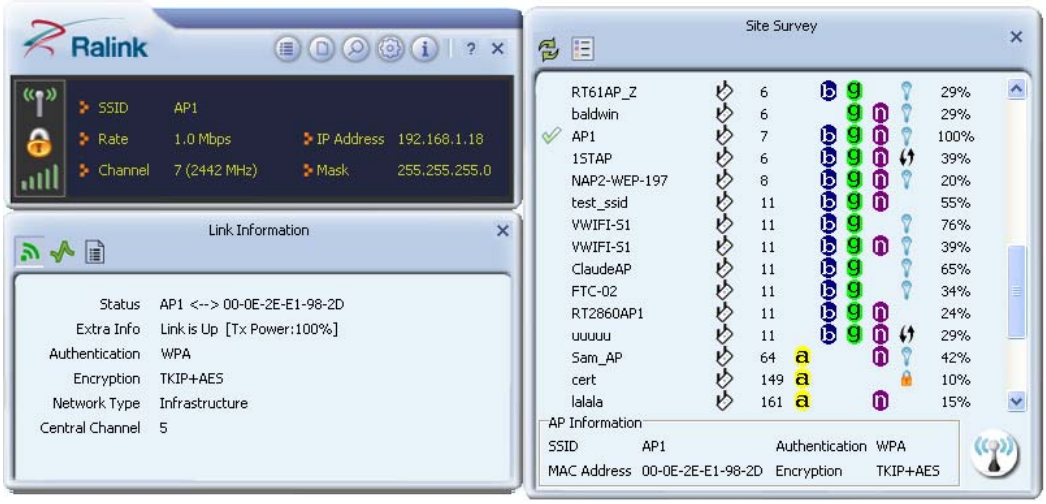


2. Click "OK". The dialog box should appear as the image below.

*If you want to disconnect, please click "Cancel" on the Authentication Status function page.

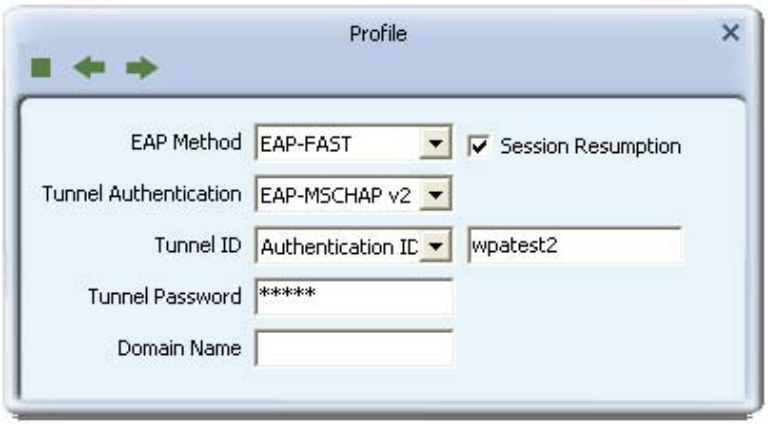
*In Profile function, show "Profile Name" option only in adding AP to Profile function.

3. If the connection is successful, the dialog box will appear as the image below.



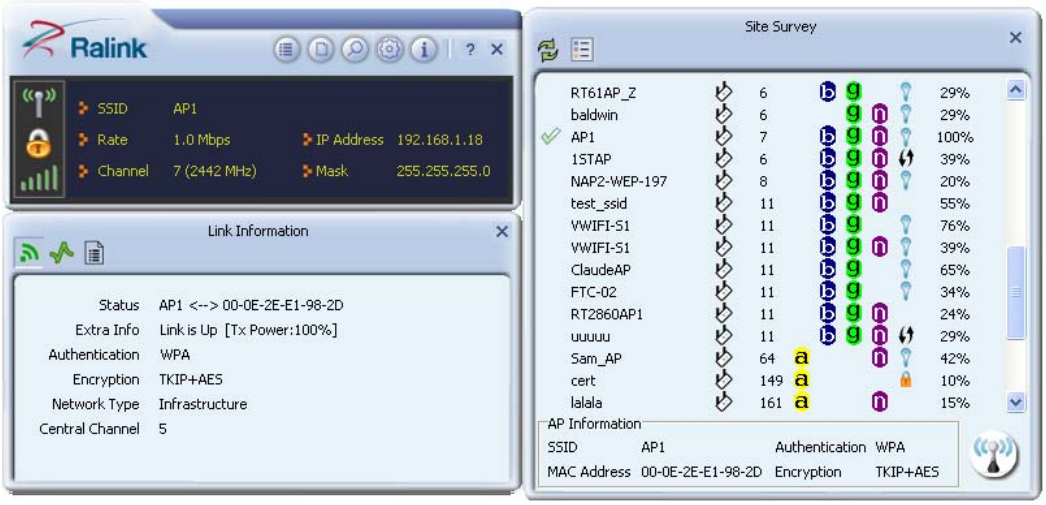
EAP-FAST:

1. Select EAP-FAST from the Authentication type drop-down list. Key-in the identity as "wpatest2" and a domain name into the blank field. The tunnel identity is "wpatest2" and password is "test2". These setting are the same as our intended AP's setting.



2. Click to the next page.

3. If the connection is successful, the dialog box will appear as the image below.



*If you want to disconnect, please click "Cancel" on the Authentication Status function page.

*In Profile function, show "Profile Name" option only in adding AP to Profile function.

4. Appendix

4.1 Country Channel List

Country channel list, channel classification and range.

Country Name	Classification	Range
Argentina	0	CH1~11
Australia	1	CH1~13
Austria	1	CH1~13
Bahrain	0	CH1~11
Belarus	1	CH1~13
Belgium	1	CH1~13
Bolivia	1	CH1~13
Brazil	0	CH1~11
Bulgaria	1	CH1~13
Canada	0	CH1~11
Chile	0	CH1~11
China	1	CH1~13
Colombia	1	CH1~13
Costa Rica	1	CH1~13
Croatia	0	CH1~11
Cyprus	1	CH1~13
Czech Republic	1	CH1~13
Denmark	1	CH1~13
Ecuador	0	CH1~11
Egypt	1	CH1~13
Estonia	1	CH1~13
Finland	1	CH1~13
France	1	CH1~13
France2	3	CH10~13
Germany	1	CH1~13
Greece	1	CH1~13
Hong Kong	0	CH1~11

Hungary	1	CH1~13
Iceland	1	CH1~13
India	1	CH1~13
Indonesia	1	CH1~13
Ireland	1	CH1~13
Israel	1	CH1~13
Italy	1	CH1~13
Japan	5	CH1~14
Japan2	4	CH14~14
Japan3	1	CH1~13
Jordan	1	CH1~13
Kuwait	1	CH1~13
Latvia	1	CH1~13
Lebanon	1	CH1~13
Latvia	1	CH1~13
Lebanon	1	CH1~13
Liechtenstein	1	CH1~13
Lithuania	1	CH1~13
Luxembourg	1	CH1~13
Macedonia	1	CH1~13
Malaysia	0	CH1~11
Mexico	0	CH1~11
Morocco	1	CH1~13
Netherlands	1	CH1~13
New Zealand	1	CH1~13
Nigeria	1	CH1~13
Norway	1	CH1~13
Panama	0	CH1~11
Paraguay	1	CH1~13
Peru	0	CH1~11
Philippines	0	CH1~11
Poland	1	CH1~13

Portugal	1	CH1~13
Puerto Rico	0	CH1~11
Romania	0	CH1~11
Russia	1	CH1~13
Saudi Arabia	0	CH1~11
Singapore	1	CH1~13
Slovakia	1	CH1~13
Slovenia	1	CH1~13
South Africa	1	CH1~13
South Korea	1	CH1~13
Spain	1	CH1~13
Sweden	1	CH1~13
Switzerland	1	CH1~13
Taiwan	0	CH1~11
Thailand	1	CH1~13
Turkey	1	CH1~13
United Arab Emirates	1	CH1~13
United Kingdom	1	CH1~13
United States of America	0	CH1~11
Uruguay	0	CH1~11
Venezuela	0	CH1~11
Yugoslavia	0	CH1~11

4.2 Acknowledgements

The above settings are used in the test platform by RaLink technology corp. Users can set the function in accordance with their AP.

Acknowledgements:

"This product includes software developed by MDC and its licensors. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)". This product includes cryptographic software written by Eric Young (eay@cryptsoft .com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

5. FAQ

5.1 FAQ

If you create an adhoc profile for 2.4G channel, and then switch wireless mode to 5G(as Figure 5-1), device will re-send beacon at the first channel of 5G. Note the original adhoc profile will keep previous settings.

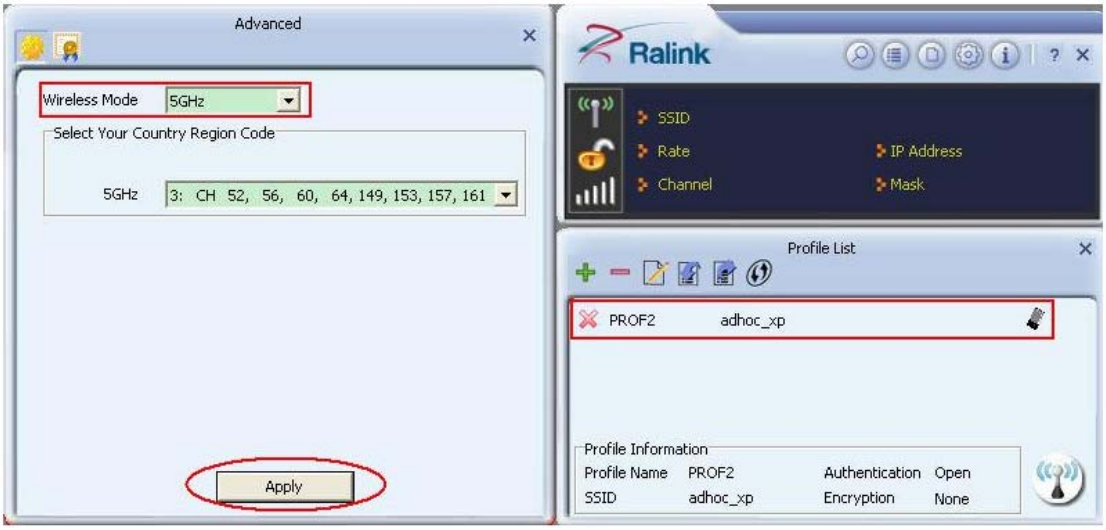


Figure 5-1 Switch wireless mode when activate an adhoc profile